F-Secure ポリシー マネージャ 7.0

管理者用ガイド

「F-Secure」および三角形のシンボルは、F-Secure Corporation の登録商標です。F-Secure の製品名およびシンボル / ロゴは、F-Secure Corporation の商標または登録商標です。本書に記載されている製品名はすべて、各社の商標または登録商標です。F-Secure Corporation は、他社の商標および名前について所有権を持つものではありません。F-Secure Corporation では、本ヘルプ中の情報の正確さを期して万全の努力を払っておりますが、情報に間違いや脱落があっても責任を負うことはありません。本書に記載されている仕様は、予告なしに変更されることがあります。

本書の例で使われている会社、名前、およびデータは、特に断りがない限り、事実とは関係ありません。本書のどの部分も、いかなる形態または手段（ 電子的または機械的 ）によっても、目的を問わず、F-Secure Corporation の書面による許可なしに複製または伝達することはできません。

本製品は以下の F-Secure の特許で保護されていることがあります。

GB2353372　GB2366691　GB2366692　GB2366693　GB2367933　GB2368233
GB2374260

Copyright © 2006 F-Secure Corporation. All rights reserved.

12000013-6J05

目次

本書について 9

概要 10
本書の構成 11
F-Secure の取扱説明書 / ガイドで使用されている記号、フォントおよび用語について . 9
記号 9

第 1 章 はじめに 11

1.1 概要 12
1.2 インストールの順序 14
1.3 機能 15
1.4 ポリシーベース管理 16
1.4.1 マネージメント インフォメーション ベース 18

第 2 章 システム要件 21

2.1 F-Secure ポリシー マネージャ サーバ 22
2.2 F-Secure ポリシー マネージャ コンソール 23

第 3 章 F-Secure ポリシー マネージャ サーバのインストール 25

3.1 概要 26
3.2 セキュリティに関する問題 27
3.2.1 F-Secure ポリシー マネージャを高度なセキュリティ環境にインストールする28
3.3 インストールの手順 33

3.4 F-Secure ポリシー マネージャ サーバの設定 48
3.4.1 通信ディレクトリのパスの変更 48
3.4.2 サーバが要求をリッスンするポートの変更 49
3.4.3 F-Secure ポリシー マネージャ サーバの設定 50
3.5 F-Secure ポリシー マネージャ サーバのアンインストール 56

第 4 章 通信ディレクトリの移行 57
4.1 はじめに 58
4.2 移行の手順 58

第 5 章 F-Secure ポリシー マネージャ コンソールのインストール 63
5.1 概要 64
5.2 インストールの手順 64
5.3 F-Secure ポリシー マネージャ コンソールのアンインストール 82

第 6 章 F-Secure ポリシー マネージャ コンソールの使用 83
6.1 概要 84
6.2 F-Secure ポリシー マネージャ コンソールの基本機能 85
6.2.1 ログイン 86
6.2.2 ユーザ インタフェース 89
6.2.3 [ポリシー ドメイン] ウィンドウ 90
6.2.4 [プロパティ] ウィンドウ 90
6.2.5 [製品ビュー] ウィンドウ 91
6.2.6 [メッセージ] ウィンドウ 98
6.2.7 ツールバー 99
6.2.8 メニュー コマンド 101
6.3 F-Secure クライアント セキュリティの管理 103
6.4 ドメインとホストの管理 104
6.4.1 ポリシー ドメインの追加 105
6.4.2 ホストの追加 106
6.4.3 ホストのプロパティ 111
6.5 ソフトウェアの配布 114
6.5.1 F-Secure によるインストール情報の送信 116
6.5.2 ポリシー ベース インストール 123
6.5.3 設定済みのパッケージを使用したローカル インストールおよび更新 128

6.5.4 情報の転送 . . . 133
6.6 ポリシーの管理 . . . 134
6.6.1 設定 . . . 134
6.6.2 制約 . . . 135
6.6.3 現在のポリシー データの保存 . . . 137
6.6.4 ポリシー ファイルの配布 . . . 137
6.6.5 ポリシーの継承 . . . 137
6.7 操作とタスクの管理 . . . 140
6.7.1 操作 . . . 140
6.8 警告の送信 . . . 141
6.8.1 警告とレポートの表示 . . . 141
6.8.2 警告転送の設定 . . . 142
6.9 レポート ツール . . . 143
6.9.1 [ポリシー ドメイン/ホスト セレクタ] ウィンドウ . . . 144
6.9.2 [レポート タイプ セレクタ] ウィンドウ . . . 145
6.9.3 [レポート] ウィンドウ . . . 146
6.9.4 下部のウィンドウ . . . 147
6.10 一般設定 . . . 148
6.10.1 接続固有の一般設定 . . . 149
6.10.2 共有一般設定 . . . 152
第 7 章 F-Secure ポリシー マネージャ サーバのメンテナンス 155
7.1 概要 . . . 156
7.2 F-Secure ポリシー マネージャ コンソール データのバックアップと復元 . . . 156
7.3 イメージファイルを使用したソフトウェアの複製 . . . 159
第 8 章 F-Secure パターン ファイルの更新 161
8.1 F-Secure 自動更新エージェントによる自動更新 . . . 162
8.1.1 F-Secure 自動更新エージェントの使用 . . . 164
8.1.2 F-Secure 自動更新エージェントのトラブルシューティング . . . 170
8.2 F-Secure ポリシー マネージャ プロキシによる自動更新 . . . 176
第 9 章 Linux 上での F-Secure ポリシー マネージャ 177
9.1 概要 . . . 178
9.1.1 Windows 版と Linux 版の違い . . . 178

9.1.2 対応ディストリビューション 178
9.2 インストール 178
9.2.1 F-Secure 自動更新エージェントのインストール 179
9.2.2 F-Secure ポリシー マネージャ サーバのインストール 179
9.2.3 F-Secure ポリシー マネージャ コンソールのインストール 180
9.2.4 F-Secure ポリシー マネージャ Web レポートのインストール 181
9.3 設定 182
9.4 アンインストール 182
9.4.1 F-Secure ポリシー マネージャ Web レポートのアンインストール 183
9.4.2 F-Secure ポリシー マネージャ コンソールのアンインストール 183
9.4.3 F-Secure ポリシー マネージャ サーバのアンインストール 184
9.4.4 F-Secure 自動更新エージェントのアンインストール 184
9.5 FAQ（よくある質問） 185

第 10 章 Web レポート 189

10.1 概要 190
10.2 はじめに 190
10.3 Web レポート クライアントのシステム要件 191
10.4 レポートの生成および表示 191
10.4.1 Web レポートの表示に必要なブラウザの設定 192
10.4.2 レポートの生成 193
10.4.3 印刷可能なレポートの作成 195
10.4.4 自動化されたレポートの生成に使用する固有の URL の生成 196
10.5 Web レポートの管理 196
10.5.1 Web レポートの無効化 197
10.5.2 Web レポートの有効化 197
10.5.3 Web レポートへの幅広いアクセスの制限または許可 198
10.5.4 Web レポートのポートの変更 199
10.5.5 Web レポート データベースのバックアップ コピーの作成 200
10.5.6 バックアップ コピーからの Web レポート データベースの復元 201
10.5.7 Web レポート データベースの最大保存期間の変更 201
10.6 Web レポートのエラー メッセージおよびトラブルシューティング 202
10.6.1 エラー メッセージ 202
10.6.2 トラブルシューティング 204

第 11 章 F-Secure ポリシー マネージャ プロキシ 205
11.1 概要 206
11.2 アンチウィルス プロキシとポリシー マネージャ プロキシの違い 206
第 12 章 トラブルシューティング 209
12.1 概要 210
12.2 FAQ（よくある質問） 210
付録 A SNMP サポート 217
A-1 概要 218
A-1.1 F-Secure ä«óùÉGÅ[ÉWÉFÉìÉgópÇÃ SNMP ÉTÉ|Å[Ég 218
A.2 SNMP サポートを含む F-Secure 管理エージェントのインストール 219
A-2.1 F-Secure SNMP ä«óùÉGÉNÉXÉeÉìÉVÉáÉìÇÃÉCÉìÉXÉgÅ[Éã 219
A.3 SNMP マスター エージェントの設定 220
A.4 マネージメント インフォメーション ベース (MIB) 221
付録 B llaunchr のエラー コード 223
B.1 概要 224
B.2 エラー コード 225
付録 C FSII リモート インストールのエラー コード 229
C.1 概要 230
C.2 Windows エラー コード 230
C.3 エラー メッセージ 231
付録 D Windows 98/ME でのリモート インストールのサポート 233
D.1 リモート管理の有効化 234
付録 E ネットマスクに使用する NSC 表記 237
E.1 概要 238
テクニカル サポート 241
概要 242

Web Club 242
Web 上でのウィルス説明 242
高度なテクニカル サポート 242
F-Secure 製品技術研修 243
研修プログラム 243
問い合わせ先 244
用語集 245
F-Secure Corporation について

本書について

概要 10
本書の構成 11

概要

F-Secure ポリシー マネージャには、以下の F-Secure ソフトウェア製品を管理するためのツールを提供します。

- F-Secure クライアント セキュリティ
- F-Secure インターネット ゲートキーパー
- F-Secure VPN+
- 以下のための F-Secure アンチウィルス :
  - ワークステーション
  - ファイアウォール
  - ファイル サーバ
  - Microsoft Exchange
  - MIMEsweeper

本書の構成

本管理者用ガイド『 F-Secure ポリシー マネージャ』は以下の章に分かれています。

第 1 章 -『はじめに』
ポリシーベース管理のアーキテクチャおよびコンポーネントについて説明します。

第 2 章 -『システム要件』
F-Secure ポリシー マネージャ コンソールと F-Secure ポリシー マネージャ サーバのソフトウェアとハードウェア要件について説明します。

第 3 章 -『F-Secure ポリシー マネージャ サーバのインストール』
F-Secure ポリシー マネージャ サーバのインストールについて説明します。

第 4 章 -『通信ディレクトリの移行』
通信ディレクトリから F-Secure ポリシー マネージャ サーバ ベースのシステムへの移行について説明します。

第 5 章 -『F-Secure ポリシー マネージャ コンソールのインストール』
F-Secure ポリシー マネージャ コンソールのアプリケーションのインストールについて説明します。

第 6 章 -『F-Secure ポリシー マネージャ コンソールの使用』
F-Secure ポリシー マネージャ コンソールの概要、セットアップ手順、ログオン手順、メニュー コマンド、および基本機能について説明します。

第 7 章 -『F-Secure ポリシー マネージャ サーバのメンテナンス』
バックアップ手順および復元方法について説明します。

第 8 章 -『F-Secure パターン ファイルの更新』
パターン ファイルを更新する様々な方法について説明します。

第 9 章 -『Linux 上での F-Secure ポリシー マネージャ』
Linux 上での F-Secure ポリシー マネージャの使用に関する情報と操作について説明します。

第 10 章 – 『Web レポート』
F-Secure ポリシー マネージャ サーバの企業向け視覚的レポート システムである F-Secure ポリシー マネージャ Web レポートの使用法について説明します。

第 11 章 – 『F-Secure ポリシー マネージャ プロキシ』
F-Secure Policy Manager Proxy の概要を説明します。

第 12 章 – 『トラブルシューティング』
トラブルシューティング情報と FAQ（よくある質問）があります。

付録 A – 『SNMP サポート』
SNMP サポートについて説明します。

付録 B – 『Ilaunchr のエラー コード』
Ilaunchr のエラー コードの一覧表です。

付録 C – 『FSII リモート インストールのエラー コード』
「Windows ホストの自動検出」の動作時に発生する可能性がある最も一般的なエラー コードおよびメッセージについて説明します。

付録 D – 『Windows 98/ME でのリモート インストールのサポート』
Windows 98/ME を使用しているワークステーションで FSII を使用するために必要な要件について説明します。

付録 E – 『ネットマスクに使用する NSC 表記』
ネットマスクに使用する NSC 表記を定義し、説明します。

用語集 – 用語について説明します。

テクニカル サポート – Web Club およびサポートの連絡先を記載しています。

About F-Secure Corporation – 会社の概要と製品を紹介します。

F-Secure の取扱説明書 / ガイドで使用されている記号、フォントおよび用語について

ここでは、本書で使用されている記号、フォントおよび用語について説明します。

記号

注意書： データの破損や復元できないことが生じる可能性を示します。

重要： 注意事項と重要な情報を示します。

参考 ： 関連情報が記載されている参照先を示します。

参照 ： 追加情報を示します。

ヒント ： 機能をより速くまたは簡単に実行にするための情報を示します。

–> 1 つの手順で完了する操作を示します。

フォント

MS ゴシック 太字（青）は、ボタンやダイアログ ボックスで使用されているメニューとコマンド名を示します。

Courier New は、コンピュータの画面に表示されるメッセージを示します。

Courier New bold は、入力が必要の情報を示します。

SMALL CAPS（黒）はキーボードのキーまたは複数のキーの組み合わせを示します。

MS ゴシック 下線（青）はユーザインターフェースのリンクを示します。

PDF ファイル

本書は PDF（Portable Document Format）ファイル形式で提供されています。Adobe Acrobat Reader を使用して、PDF ファイルを表示および印刷できます。印刷する際には、著作権と免責条項文を含むすべてのページを印刷するようにお願いします。

追加情報

F-Secure の Web サイト（http://www.f-secure.co.jp）にアクセスすると、マニュアル、トレーニングコース、ダウンロードおよびサポートとサービス情報をご覧になれます。

F-Secure の文献を今後改善し続けるために、よろしければ、お客様のフィードバックをぜひお聞かせください。本書または F-Secure の他の文献にご質問、ご意見、ご提案などございましたら、documentation@f-secure.com までどうぞご連絡ください。

1 はじめに

概要 12
インストールの順序 14
機能 15
ポリシーベース管理 16

1.1 概要

F-Secure ポリシー マネージャは、ネットワーク上に分散している複数のオペレーティング システム上の多数のアプリケーションのセキュリティ ポリシーやパターン ファイルを処理および拡張できる、一元集中管理ソフトウェアです。ポリシー マネージャを使用することによって、セキュリティ ソフトウェアを常に最新の状態に更新したり、ネットワークとホストの構成を状況に応じて管理したり、企業コンプライアンスを監視したりすることなどが可能になります。また、大規模のネットワークやモバイル ユーザが混雑するシステムにも柔軟に対応することができます。F-Secure ポリシー マネージャは、セキュリティ ポリシーの定義、ローカルおよびリモート システムへのポリシーの配布とアプリケーションのインストール、企業内の全システムのアクティビティを監視して、それらが企業ポリシーに従って一元集中管理されていることを確認するための、統合化された堅牢なインフラストラクチャを提供します。

F-Secure 自動更新エージェントは、F-Secure ポリシー マネージャ サーバの一部としてインストールすることができます。

F-Secure ポリシー マネージャは、F-Secure の管理アーキテクチャを採用しているため、広域に分散化されているモバイル システムに強力な拡張性を提供します。F-Secure ポリシー マネージャは、F-Secure ポリシー マネージャ コンソールと F-Secure ポリシー マネージャ サーバで構成されています。これらは、ローカル ホストでのすべての管理機能を処理する F-Secure 管理エージェントに、シームレスに統合されています。

F-Secure ポリシー マネージャの主要コンポーネント

F-Secure ポリシー マネージャ コンソールには、ネットワーク内の管理ホストのセキュリティを管理する集中管理コンソールが用意されています。これによって、管理者は、ネットワークを論理単位に編成してポリシーを共有することができます。これらのポリシーは、F-Secure ポリシー マネージャ コンソールで定義され、F-Secure ポリシー マネージャ サーバを通じてワークステーションへ配布されます。F-Secure ポ

リシー マネージャ コンソールは、Java ベースのアプリケーションで、複数のプラットフォーム上で実行できます。ローカル ログイン スクリプト、再起動などのエンドユーザによる操作を必要とせずに、管理エージェントを他のワークステーション上にリモート操作でインストールすることができます。

F-Secure ポリシー マネージャ サーバは、管理者から配布されるポリシーやソフトウェア パッケージ用、および管理されたホストから送信されるステータス情報や警告用のリポジトリです。Apache Web サーバの拡張機能として動作することによって、拡張性を提供します。F-Secure ポリシー マネージャ サーバと管理対象ホスト間の通信は、標準の HTTP プロトコルを介して行われるため、LAN および WAN のネットワーク パフォーマンスには影響しません。

F-Secure ポリシー マネージャ Web レポートは、F-Secure ポリシー マネージャ サーバに付属する、Web ベースの視覚的レポート システムです。F-Secure ポリシー マネージャ Web レポートを使用すると、過去のデータにや傾向に基づいて視覚的なレポートをすばやく作成し、ウィルス発生に対して保護されていないコンピュータや被害を受けやすいコンピュータを識別することができます。

F-Secure ポリシー マネージャ レポート オプションはスタンドアロンのコマンドライン プログラムで、F-Secure ポリシー マネージャ サーバの既存の通信ディレクトリ（CommDir）を使用して、選択した管理対象のセキュリティ ドメインやホストから、警告、ステータス、およびプロパティのデータを収集します。F-Secure ポリシー マネージャ レポート オプションによって、ユーザは F-Secure ポリシー マネージャ サーバの通信ディレクトリのデータに関するレポートを、定義済みのクエリーに似た XSL テンプレートを使用して生成できます。これらのレポートは、HTML、XML、CSV、または TXT 形式のファイルとしてエキスポートすることが可能です。

F-Secure ポリシー マネージャ更新サーバおよびエージェントは管理対象ホストのウィルス パターン ファイルとスパイウェアの定義ファイルを更新するために使用します。F-Secure 自動更新エージェントによって、ユーザは Web からファイルをダウンロードするために作業を中断することなく、自動更新や情報コンテンツを受信することができます。F-Secure 自動更新エージェントは他のインターネット アプリケーションで使用されていない帯域幅を使用して、ファイルを透過的および自動的にダウンロードします。これによってユーザはウィルスおよびスパイウェアの保護ファイルの最新版を容易に入手することができます。

F-Secure 自動更新エージェントがインターネットに常時接続されている場合、クライアントは新しいパターン ファイルを、F-Secure が発行してから約 2 時間後に自動的に受け取れるように設定できます。

F-Secure 管理エージェントは、管理者が管理ホストに設定したセキュリティ ポリシーを実施し、エンドユーザにユーザ インタフェースおよびその他のサービスを提供します。管理エージェントは、ローカル ワークステーションのすべての管理機能を処理し、すべての F-Secure アプリケーションに対して共通のインタフェースを提供し、ポリシー ベースの管理インフラストラクチャ内で動作します。

VPN+ 認証ウィザードは F-Secure VPN+ に証明書を作成するアプリケーションです。

1.2 インストールの順序

F-Secure ポリシー マネージャをインストールするには、次のインストール順序に従ってください（F-Secure ポリシー マネージャ サーバと F-Secure ポリシー マネージャ コンソールを同じマシンにインストールする場合を除きます。この場合、セットアップが同じインストール プロセスですべてのコンポーネントをインストールします）。

1. F-Secure ポリシー マネージャ サーバおよび F-Secure ポリシー マネージャ更新サーバおよびエージェント
2. F-Secure ポリシー マネージャ コンソール
3. 管理対象の各アプリケーション

1.3 機能

ソフトウェアの配布

- F-Secure のインストール情報の送信を使用した、Windows ドメインへの最初のインストール。
- パターン ファイルを含む、実行可能ファイルおよびデータ ファイルの更新。
- ポリシーベースの更新のサポート。ポリシーに従って、F-Secure 管理エージェントはホスト上で更新を行います。ポリシーおよびソフトウェア パッケージの両方が署名されるため、更新処理全体が強力に認証され、安全になります。
- 更新は、以下の複数の方法で実行できます。
  - F-Secure CD の利用。
  - F-Secure Web サイトからユーザに対して提供。F-Secure 自動更新エージェントによって自動的に「プッシュ」する方法と、F-Secure Web サイトから自発的に「プル」する方法があります。
- F-Secure ポリシー マネージャ コンソールを使用して、設定済みのインストール パッケージをエキスポートすることができます。インストール パッケージは、SMS などのサードパーティ製ソフトウェアや同様のツールを使用してエキスポートすることもできます。

設定とポリシー管理

- セキュリティ ポリシーの設定の集中化。管理者は、F-Secure ポリシー マネージャ サーバからユーザのワークステーションにポリシーを配布します。ポリシーの保全性は、電子署名の使用によって保証されます。

イベント管理

- 管理 API を介した、イベント ビューア（ローカル ログとリモート ログ）、SNMP エージェント、電子メール、レポート ファイルなどへのレポート
- ポリシーによるイベントのリダイレクト
- イベントの統計情報

パフォーマンス管理

- 統計情報とパフォーマンス データの処理およびレポート

タスク管理

- ウィルス スキャン タスクなどの操作の管理

1.4 ポリシーベース管理

セキュリティ ポリシーは、機密情報などのリソースの管理、保護、および配布方法を明確に定めた一連のルールです。F-Secure ソフトウェアの管理アーキテクチャは、企業環境での最適なセキュリティ管理のために、管理者が集中設定したポリシーを使用します。ポリシーベース管理で、以下のような多くの機能が実行されます。

- 製品の動作のリモート制御およびモニタリング
- 製品および管理エージェントから提供される統計情報のモニタリング
- 定義済み操作のリモート起動
- 製品からの警告および通知のシステム管理者への転送

F-Secure ポリシー マネージャ コンソールとホスト間の情報交換は、ポリシー ファイルを転送することによって行われます。ポリシー ファイルには、以下の 3 種類があります。

- デフォルト ポリシー ファイル（.dpf）
- ベース ポリシー ファイル（.bpf）
- インクレメンタル ポリシー ファイル（.ipf）

製品の現在の設定は、この 3 種類のポリシー ファイルで構成されます。

デフォルト ポリシー ファイル

デフォルト ポリシー ファイルには、セットアップ プログラムによってインストールされた 1 つの製品のデフォルト値が含まれます。デフォルト ポリシーは、ホストでのみ使用されます。ベース ポリシー ファイルとインクレメンタル ポリシー ファイルのどちらにも変数のエントリがない場合、デフォルト ポリシー ファイルの値が使用されます。各製品に専用のデフォルト ポリシー ファイルがあります。新しいバージョンの製品には、デフォルト ポリシー ファイルの新しいバージョンが含まれています。

ベース ポリシー ファイル

ベース ポリシー ファイルには、特定のホストにある F-Secure 製品のすべての変数の管理設定および制約が含まれます（ドメイン レベルのポリシーでは、ホスト グループが同じファイルを共有する場合があります）。ベース ポリシー ファイルは F-Secure ポリシー マネージャ コンソールにより署名され、ネットワークを通過している間およびホストのファイル システムに格納されている間、変更されないように保護されます。これらのファイルは、F-Secure ポリシー マネージャ コンソールから F-Secure ポリシー マネージャ サーバに送信されます。ホストは、F-Secure ポリシー マネージャ コンソールにより作成された新規ポリシーを定期的にポーリングします。

インクレメンタル ポリシー ファイル

インクレメンタル ポリシー ファイルは、ベース ポリシーに対してローカルに行った変更を保存するために使用されます。ベース ポリシーで指定された制限範囲内であれば、変更が可能です。インクレメンタル ポリシー ファイルは、管理者が現在の設定と統計を参照できるように、定期的に F-Secure ポリシー マネージャ コンソールへ送信されます。

1.4.1 マネージメント インフォメーション ベース

MIB (Management Information Base : マネージメント インフォメーション ベース) は、SNMP (Simple Network Management Protocol : 簡易ネットワーク管理プロトコル) で使用される階層管理用のデータ構造です。F-Secure ポリシー マネージャでは、ポリシー ファイルの内容を定義するために MIB 構造が使用されます。個々の変数には、オブジェクト識別子 (OID) と、ポリシー API を使用してアクセスできる値があります。F-Secure MIB の概念には、SNMP MIB の基本的な定義に加え、完璧なポリシーベース管理を実現するのに必要な数多くの拡張機能が含まれています。

以下のカテゴリが製品の MIB で定義されます。

設定	SNMP 方式でのワークステーション管理に使用されます。管理される製品の動作は、このカテゴリで指定された内容によって制限されます。
統計情報	製品の統計情報を F-Secure ポリシー マネージャ コンソールへ送信します。
操作	操作は 2 つのポリシー変数で処理されます。1 つは操作の識別子をホストへ転送する変数で、もう 1 つは実行された操作を F-Secure ポリシー マネージャ コンソールに通知する変数です。後者の変数は通常の統計情報を使用して転送され、前に行われた操作すべてが同時に認識されます。操作を編集するカスタム エディタはサブツリーに関連付けられており、2 つの変数はエディタでは非表示になります。
プライベート	管理概念 MIB には、セッション間の内部使用のために製品が保存する変数も含まれています。これにより、製品は Windows レジストリ ファイルのような外部のサービスに依存する必要はなくなります。

トラップ	トラップとは、ローカル コンソール、ログ ファイル、リモート管理プロセスなどに送られる、警告やイベントなどのメッセージです。ほとんどの F-Secure 製品が、以下のタイプのトラップを送信します。
	情報。ホストからの通常の操作情報です。
	警告。ホストからの警告です。
	エラー。ホスト上の回復可能なエラーです。
	重大なエラー。ホスト上の回復不可能なエラーです。
	セキュリティ警告。ホスト上のセキュリティ危険要因です。

2 システム要件

F-Secure ポリシー マネージャ サーバ 22
F-Secure ポリシー マネージャ コンソール 23

2.1 F-Secure ポリシー マネージャ サーバ

F-Secure ポリシー マネージャ サーバをインストールするには、お使いのシステムが少なくとも次の要件を満たしている必要があります。

オペレーティング システム：	**Microsoft Windows** Microsoft Windows 2000 Server (SP 3 以降)、Windows 2000 Advanced Server (SP 3 以降)、Windows Server 2003、Standard Edition または Web Edition、Windows 2003 Small Business Server **Linux** Red Hat Enterprise Linux 4 Red Hat Enterprise Linux 3 SUSE Linux 10.0 SUSE Linux 9.x SUSE Linux Enterprise Server 9 Debian GNU Linux Sarge 3.1
プロセッサ：	Intel Pentium III 450 MHz 以上のプロセッサ。5000 台を超えるホストの管理または Web レポートの使用には、Intel Pentium III 1 GHz 以上のプロセッサが必要。
メモリ：	256 MB RAM。 Web レポートが有効の場合には、512 MB RAM。
ディスク容量：	200 MB のディスク容量が必要。500 MB 以上を推奨。必要なディスク容量は、インストールのサイズによって異なる。 この容量に加え、警告およびポリシー用として各ホストに約 1 MB を割り当てることを推奨。ポリシーの使用方法と格納されるインストールパッケージの数によってディスク使用量は異なることから、ホストごとの実際のディスク使用量を予測することは困難。
ネットワーク：	10 Mbit ネットワーク。5000 台を超えるホストの管理には、100 Mbit のネットワークが必要。

2.2 F-Secure ポリシー マネージャ コンソール

F-Secure ポリシー マネージャ コンソールをインストールするには、お使いのシステムが少なくとも次の要件を満たしている必要があります。

オペレーティング システム：	**Microsoft Windows** Microsoft Windows 2000 Professional (SP 以降) Windows 2000 Server (SP3 以降) Windows 2000 Advanced Server (SP3 以降) Windows XP Professional (SP2 以降) Windows Server 2003、Standard Edition または Web Edition Windows 2003 Small Business Server **Linux** Red Hat Enterprise Linux 4 Red Hat Enterprise Linux 3 SUSE Linux 10.0 SUSE Linux 9.x SUSE Linux Enterprise Server 9 Debian GNU Linux Sarge 3.1
プロセッサ：	Intel Pentium III 450 MHz 以上のプロセッサ。5000 台を超えるホストの管理には、Pentium III 750 MHz 以上のプロセッサが必要。
メモリ：	256 MB RAM。 5000 台以上のホストの管理には、512MB RAM。

ディスク容量 ：	100 MB のディスク容量。
ディスプレイ ：	解像度 1024x768、256 色以上を表示可能なディスプレイ（解像度 1280x960 以上で 32 ビット カラーを推奨）。
ネットワーク ：	Ethernet ネットワーク インタフェースまたは同等のインタフェース。 コンソールとサーバの間には 10 Mbit 以上のネットワークを推奨。5000 台を超えるホストの管理には、コンソールとサーバの間に 100 Mbit の接続が必要。

3 F-SECURE ポリシー マネージャ サーバのインストール

概要 26
セキュリティに関する問題 27
インストールの手順 33
F-Secure ポリシー マネージャ サーバのアンインストール 56

3.1 概要

ここでは、サーバ専用のコンピュータに F-Secure ポリシー マネージャ サーバをインストールする詳細な手順を説明します。F-Secure ポリシー マネージャ サーバは、F-Secure ポリシー マネージャ コンソールと同じマシンにインストールすることもできます。

F-Secure ポリシー マネージャ サーバは F-Secure ポリシー マネージャ コンソールと管理対象ホストを結ぶもので、管理者が配布するポリシーやソフトウェア パッケージのリポジトリとしてだけでなく、管理されているホストが送信するステータス情報や警告のリポジトリとしても機能します。

F-Secure ポリシー マネージャ サーバと他のコンポーネントの間の通信は標準の HTTP プロトコルを介して実行されますので、LAN および WAN のネットワーク パフォーマンスは影響されません。

F-Secure ポリシー マネージャ サーバが保存する情報には、以下のファイルがあります。

- ポリシー ドメイン構造
- 各ポリシー ドメインまたはホストに与えられる実際のポリシー情報であるポリシー データ
- ポリシー データから生成されたベース ポリシー ファイル
- インクレメンタル ポリシー ファイル、警告、レポートなどのステータス情報
- ホストから送信される自動登録要求
- PKCS#10 証明要求（F-Secure VPN+ のみ）
- ホスト証明書
- F-Secure から受信するセキュリティ ニュース
- 製品のインストールおよびパターン ファイル更新パッケージ
- ホストに関する統計および過去の傾向データなどを保管する Web レポート コンポーネント

本書では F-Secure ポリシー マネージャ レポート オプションについては説明しません。このコンポーネントの詳細については、『F-Secure ポリシー マネージャ レポート オプション管理者用ガイド』を参照してください。

3.2 セキュリティに関する問題

F-Secure ポリシー マネージャ サーバは Apache Web サーバ技術を使用しています。本製品には安全かつ最新の技術を使用するよう全力で取り組んでいますが、Apache の技術やセキュリティに関する情報を次のサイトで定期的に確認することを推奨します。

オペレーティング システムや Apache Web サーバに関するセキュリティ上の問題の情報は CERT の Web サイト（http://www.cert.org）で参照できます。

インストールした Apache Web サーバのセキュリティを確保する方法を説明した文書については、http://www.apache.org/docs/misc/security_tips.html で参照できます。また、脆弱性のリストについては、http://www.apacheweek.com/features/security-13 で参照できます。

リリース ノートには、インストールおよびセキュリティに関する重要な情報が記載されているので、必ずお読みください。

3.2.1 F-Secure ポリシー マネージャを高度なセキュリティ環境にインストールする

F-Secure ポリシー マネージャは、企業内ネットワークにおいて主に F-Secure アンチウィルス製品の管理に使用することを目的として設計されています。F-Secure ポリシー マネージャをインターネットなどの公共ネットワーク上で使用することは推奨しません。

重要 : 高度なセキュリティ環境で F-Secure ポリシー マネージャをインストールする場合は、管理ポート（デフォルトでは 8080）とホストのポート（デフォルトでは 80）がインターネットに表示されないようにしてください。

F-Secure ポリシー マネージャの組み込みのセキュリティ機能

F-Secure ポリシー マネージャには、ポリシー ドメイン構造やポリシー データの変更を確実に検出するためのセキュリティ機能が組み込まれています。さらに重要なことに、管理対象ホストに不正な変更を展開することはできません。これらの両機能は、管理者しか使用できない管理用鍵ペアに依存しています。これらの機能は強力なデジタル署名に基づいており、多くの場合は、ほとんどのアンチウィルス製品インストール環境において使いやすさとセキュリティの適度なバランスを保つことができます。ただし、高度なセキュリティ環境では、次の機能には追加設定が必要になる場合があります。

1. デフォルトでは、すべてのユーザがポリシー マネージャ サーバに読み取り専用モードでアクセスできますが、表示できるのは管理データだけです。これにより、完全な管理者権限のないユーザとの間でも情報共有が容易になります。複数のユーザが読み取り専用

セッションを同時に開いて、システムのステータスを監視することができます。他の管理者や管理対象ホストへの影響はまったくありません。

2. 新しい管理用鍵に簡単に移行できるようにするため、新しく作成された鍵ペアや既存の鍵ペアを使用して、ポリシー ドメイン構造とポリシー データに再署名することができます。誤って再署名した場合や、権限のないユーザが故意に再署名した場合、許可されているユーザが次に F-Secure ポリシー マネージャにログインしたときに、変更があったことがわかるようになっています。最悪の場合、許可されているユーザは、権限のないユーザによる変更を取り消すために、バックアップを復元する必要があります。いずれにしても、ポリシー ドメイン構造とポリシー データの変更は検出され、正しいオリジナルの鍵ペアがなければ、変更を管理対象ホストに配布することはできません。

管理データの参照も制限する必要がある高度なセキュリティ環境では、これらの機能は望ましくないことがあります。次の方法でシステムのセキュリティ レベルを向上できます。

高度なセキュリティ環境で可能なさまざまなインストール方法

1. F-Secure ポリシー マネージャ サーバと F-Secure ポリシー マネージャ コンソールを同じコンピュータにインストールし、F-Secure ポリシー マネージャ サーバへのアクセスをローカルホストのみに制限します。このように制限すると、F-Secure ポリシー マネージャ コンソールを使用できるのは、ローカルホストに物理的にアクセスできるユーザだけになります。

   インストール時に、F-Secure ポリシー マネージャ サーバへのアクセスをローカルホストのみに制限した場合 （手順 9. (P41) を参照）、F-Secure セットアップは `httpd.conf` ファイルの `#FSMSA listen` ディレクティブを次のように変更します。

   ```
   #FSMSA listen
       Listen 127.0.0.1:8080 <- ローカルホストから PMC ポート 8080 への接続のみを許可
   ```

2. httpd.conf ファイルを編集して、F-Secure ポリシー マネージャ サーバへのアクセスを別に定義した IP アドレスのみに制限します。

セットアップ時にポート 8080 へのアクセスをローカルホストのみに制限した場合は、ここで、そのポートを開いて、許可する IP アドレスのリストを作成する必要があります（次の Listen 8080 ディレクティブの例を参照してください）。

次に、httpd.conf ファイルの編集例を示します。

```
#FSMSA listen
Listen 8080 <- 接続がローカルホストのみに制限されていないことを確認

#FSMSA port
<VirtualHost _default_:8080>
    <Location /fsmsa/fsmsa.dll>
     Order Deny,Allow
     Deny from all                  <- まず、すべてを拒否
     Allow from 127.0.0.1 <- 続いて、ローカル マシンからサーバへのアクセスを許可
     Allow from 10.128.129.2 <- サーバ マシンからのアクセスを許可
     Allow from 10.128.129.209 <- 管理者用ワークステーションからのアクセスを許可
     SetHandler fsmsa-handler
    </Location>
</VirtualHost>
```

このようにすると、定義された IP アドレスのマシンにアクセスできるユーザだけが F-Secure ポリシー マネージャ コンソールを使用できます。

3. F-Secure ポリシー マネージャを公共のネットワーク（インターネットなど）上で使用する必要がある場合は、F-Secure ポリシー マネージャ サーバと F-Secure ポリシー マネージャ コンソールの間の接続を VPN や SSH 製品で暗号化することを推奨します。

または、F-Secure ポリシー マネージャ コンソールと F-Secure ポリシー マネージャ サーバ を同じコンピュータにインストールし、アクセスをローカルホストに制限することもできます。F-Secure ポリシー マ

ネージャ コンソールへの管理者によるリモート アクセスは、セキュリティで保護されたリモート デスクトップ製品を使用して処理することができます。

F-Secure ポリシー マネージャ Web レポートを高度なセキュリティ環境にインストールする

F-Secure ポリシー マネージャ Web レポートは、企業内ネットワークで使用して、F-Secure クライアント セキュリティのウィルス保護ステータスや警告などに関するグラフィカルなレポートを生成することを目的に設計されています。F-Secure ポリシー マネージャ Web レポートをインターネットなどの公共ネットワーク上で使用することは推奨しません。

高度なセキュリティ環境で可能なさまざまなインストール方法

1. インストール時に、Web レポートへのアクセスをローカルホストのみに制限します。このように制限すると、F-Secure ポリシー マネージャ Web レポートを使用できるのは、ローカルホストに物理的にアクセスできるユーザだけになります。

   インストール時に、F-Secure ポリシー マネージャ Web レポートへのアクセスをローカルホストのみに制限した場合（(P42) を参照）、F-Secure セットアップは httpd.conf ファイルの `#Web Reporting listen` ディレクティブを次のように変更します。

   ```
   #Web Reporting listen
   Listen 127.0.0.1:8081 <- ローカルホストから Web レポート ポート 8081 への接続のみを許可
   ```

2. httpd.conf ファイルを編集して、F-Secure ポリシー マネージャ Web レポートへのアクセスを、別に定義した IP アドレスのみに制限します（次の説明を参照してください）。

> セットアップ時にポート 8081 へのアクセスをローカルホストのみに制限した場合は、ここで、そのポートを開いて、許可する IP アドレスのリストを作成する必要があります（次の Listen 8081 ディレクティブの例を参照してください）。

次に、httpd.conf ファイルの編集例を示します。ここでは、ローカルホストと、別途定義した 1 つの IP アドレスからのアクセスを許可しています。

#Web Reporting listen

Listen 8081

Web Reporting port:

<VirtualHost _default_:8081>

JkMount /* ajp13

ErrorDocument 500 "ポリシー マネージャ サーバはポリシー マネージャ Web レポートに

アクセスできませんでした。"

<Location / >

Order Deny,Allow

Deny from all ← まず、すべて拒否

Allow from 127.0.0.1 ← 続いて、ローカル マシンから Web レポートへのアクセスを許可

Allow from 10.128.129.209 ← 管理者用ワークステーションからのアクセスを許可

</Location>

</VirtualHost>

この変更を行うと、F-Secure ポリシー マネージャ Web レポートを使用できるのは、ローカル ホスト、または定義した IP アドレスのマシンにアクセスできるユーザだけになります。

3.3 インストールの手順

F-Secure ポリシー マネージャ サーバをインストールするには、サーバとなるコンピュータに物理的にアクセスできる必要があります。

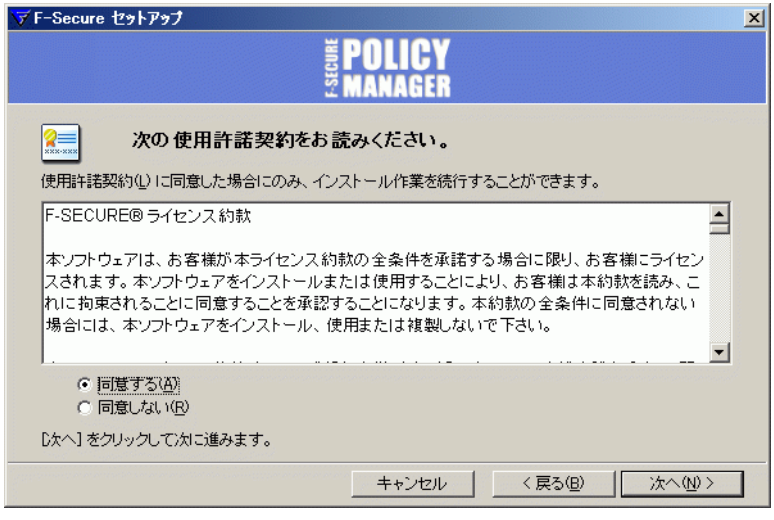
手順 1.

1. F-Secure CD を CD-ROM ドライブに入れます。
2. [企業用] を選択します。[**次へ**] をクリックして次に進みます。
3. [管理ソフトウェアのインストールまたは更新] メニューに移動して、[F-Secure ポリシー マネージャ] を選択します。

手順 2.

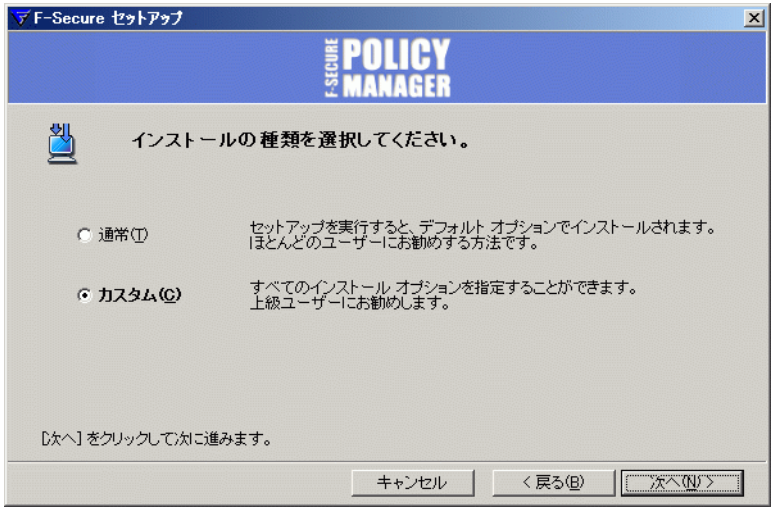
セットアップが開始されます。初期画面が表示されたら、セットアップ画面の指示に従います。ドロップダウン メニューでインストール言語を選択します。[**次へ**] をクリックして次に進みます。

手順 3. 使用許諾契約情報を読みます。同意する場合は、[同意する] を選択します。[次へ] をクリックして次に進みます。



手順 4. インストールの種類を選択します。

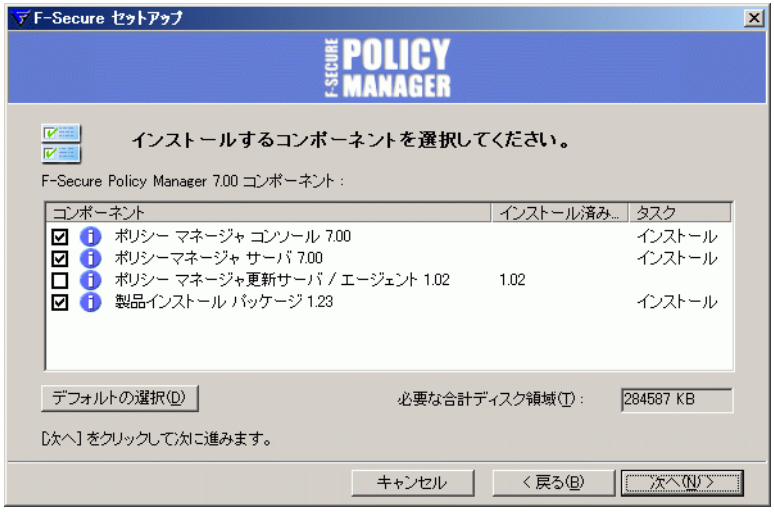
- 通常 - 製品をデフォルトのオプションでインストールします。
  - F-Secure ポリシー マネージャ サーバ、F-Secure ポリシー マネージャ コンソール、F-Secure ポリシー マネージャ更新サーバおよびエージェントが、同じコンピュータにインストールされます。
  - デフォルト ポートは F-Secure ポリシー マネージャ サーバ モジュールによって使用されます。
  - 同じコンピュータにインストールされた F-Secure ポリシー マネージャ コンソールだけが、F-Secure ポリシー マネージャ サーバにアクセスできます。
  - Web レポートへのアクセスは、他のコンピュータからも許可されます。
- カスタム - デフォルトの（推奨）オプションです。インストール先ディレクトリや F-Secure ポリシー マネージャ サーバ モジュールが使用するポートなどを指定できます。一部のダイアログは、[カスタム] を選択した場合にのみ表示されます。
- 再インストール - すべての既存のコンポーネントを再インストールし、不足している設定を復元します。このオプションは、コンピュータに F-Secure ポリシー マネージャがインストールされている場合にのみ表示されます。


F-Secure セットアップ
F-SECURE POLICY MANAGER
インストールの種類を選択してください。
通常(T)
セットアップを実行すると、デフォルト オプションでインストールされます。
ほとんどのユーザーにお勧めする方法です。
カスタム(C)
すべてのインストール オプションを指定することができます。
上級ユーザーにお勧めします。
[次へ] をクリックして次に進みます。
キャンセル
< 戻る(B)
次へ(N) >

手順 5. F-Secure コンポーネントがインストールされていないコンピュータにインストールする場合は、次のコンポーネントを選択します。

- F-Secure ポリシー マネージャ サーバ
- F-Secure ポリシー マネージャ更新サーバおよびエージェント - パターン ファイルの更新を自動化します。
- F-Secure インストール パッケージ - このオプションは、CD から新しいリモート インストール パッケージをアップロード / インストールする場合に選択します（推奨）。

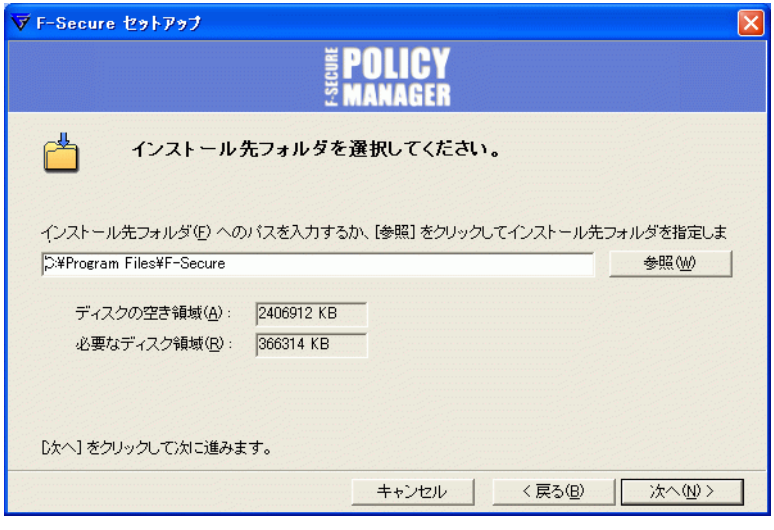
[次へ] をクリックして次に進みます。



手順 6. インストール先フォルダを選択します。[次へ] をクリックします。

デフォルトのインストール先ディレクトリを使用することを推奨します。F-Secure ポリシー マネージャ サーバを別のフォルダにインストールする場合は、[参照] をクリックして、別のフォルダを選択します。

警告 ： F-Secure 管理エージェントが同じコンピュータにインストールされている場合は、F-Secure ポリシー マネージャ サーバのインストール先ディレクトリを変更しないでください。



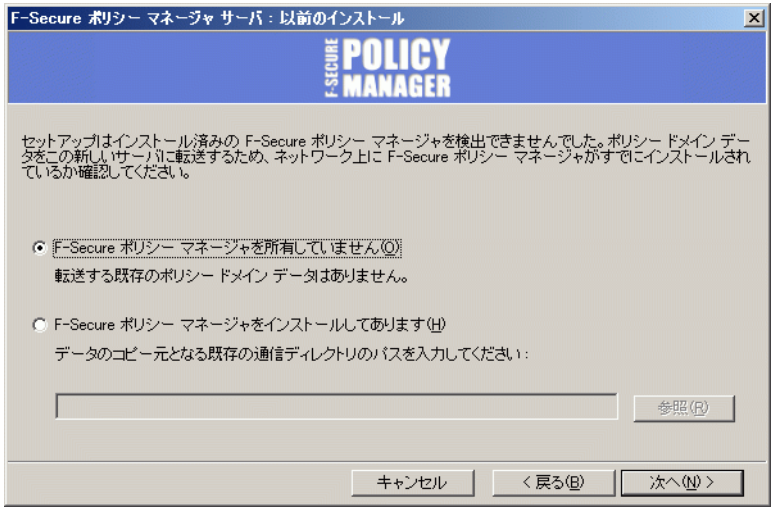
手順 7.

セットアップにより、F-Secure ポリシー マネージャの以前のバージョンがインストールされているかどうかを確認するメッセージが表示されます。

1. インストールされている場合は、[F-Secure ポリシー マネージャをインストールしてあります] を選択します。インストールされている F-Secure ポリシー マネージャの通信ディレクトリのパスを入力します。このディレクトリの内容は、<サーバのインストール先ディレクトリ>¥ 通信ディレクトリ（F-Secure ポリシー マネージャ サーバ インストール先ディレクトリの commdir¥ ディレクトリ）以下にコピーされ、F-Secure ポリシー マネージャ サーバはこのディレクトリをリポジトリとして使用します。以前の commdir をバックアップとして使用することも、F-Secure ポリシー マネージャ サーバが正しくインストールされたことを確認したら削除することもできます。
2. インストールされていない場合は、[F-Secure ポリシー マネージャを所有していません] を選択します。

   この場合、既存の commdir は必要ありません。デフォルトの場所（<F-Secure ポリシー マネージャ 5 のインストール先ディレクトリ>¥commdir）に空の通信ディレクトリが作成されます。

[**次へ**] をクリックして次に進みます。



手順 8. 既存の設定を維持するか、設定を変更するかを選択します。

このダイアログは、コンピュータにインストール済みの F-Secure ポリシー マネージャ サーバが検出された場合にのみ表示されます。

- デフォルトでは、セットアップは既存の設定を維持します。F-Secure ポリシー マネージャ サーバの構成ファイル (HTTPD.conf) を手動で更新している場合は、このオプションを選択してください。このオプションは、既存の管理、ホスト、および Web レポートのポートを自動的に維持します。
- 以前のインストールのポートを変更する場合は、[Change settings] オプションを選択します。このオプションは HTTPD.conf ファイルを上書きし、設定をデフォルトに戻します。

手順 9.

有効にする F-Secure ポリシー マネージャ サーバのモジュールを選択します。

- ホスト モジュールは、ホストとの通信に使用されます。デフォルトのポートは 80 です。
- 管理モジュールは、F-Secure ポリシー マネージャ コンソールとの通信に使用されます。デフォルトの HTTP ポートは 8080 です。

  通信用のデフォルトのポートを変更する場合も、F-Secure ポリシー マネージャ コンソールで HTTP ポート番号の設定を変更する必要があります。

  デフォルトでは、管理モジュールへのアクセスはローカル コンピュータに制限されています。これは、製品の最も安全な使用方法です。

  ネットワークでの接続を使用する場合は、F-Secure SSH または F-Secure VPN+ との通信のセキュリティ対策を検討してください。

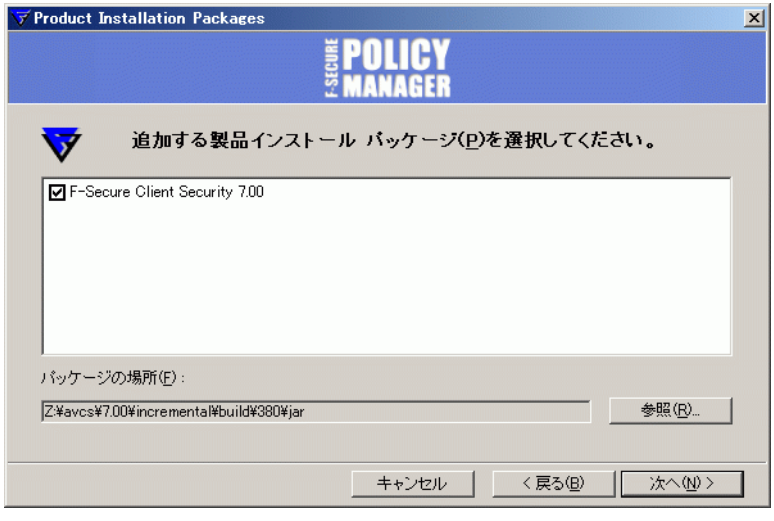
  最高のセキュリティを必要とする環境については、本書の『F-Secure ポリシー マネージャを高度なセキュリティ環境にインストールする』のセクションを参照してください。

- Web レポート モジュールは、F-Secure ポリシー マネージャ Web レポートとの通信に使用されます。有効にするかどうかを選択します。Web レポートは管理モジュールへのローカル ソケット接続を使用して、サーバ データを取り出します。デフォルトのポートは 8081 です。

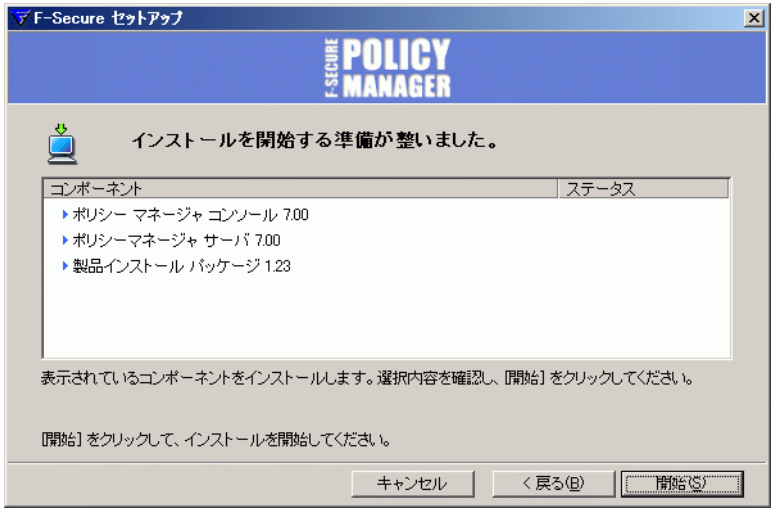
  デフォルトでは、Web レポートへのアクセスは、他のコンピュータからも許可されます。このコンピュータからのアクセスのみを許可する場合は、[アクセスをローカル マシンのみに制限する] を選択します。

［ 次へ ］をクリックして次に進みます。

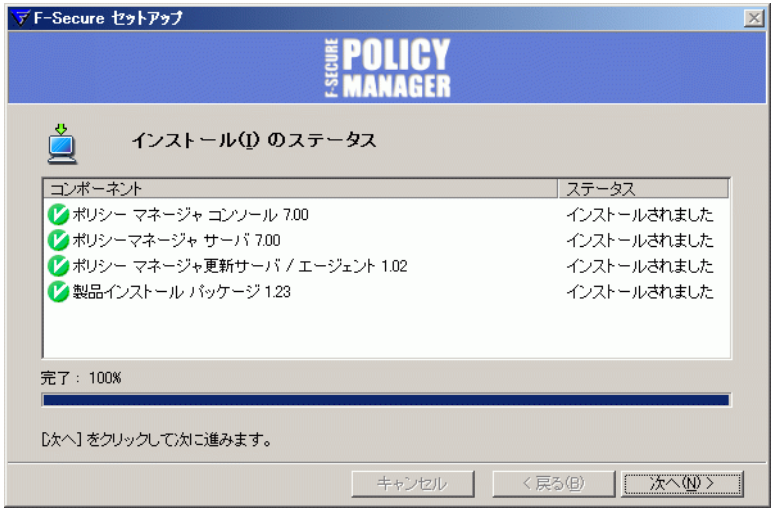
手順 10. 使用可能なパッケージのリストから、追加する製品のインストール パッケージを選択します（17 ページの手順 4 で F-Secure インストール パッケージを選択した場合）。[**次へ**] をクリックします。



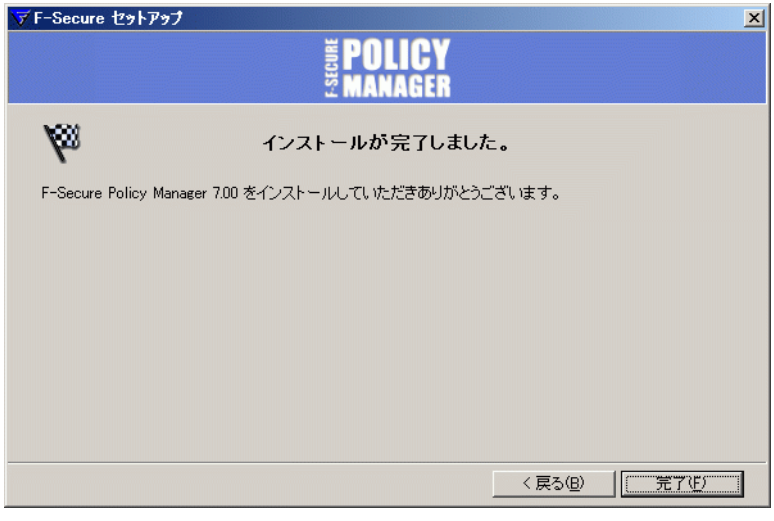
手順 11. セットアップにより、インストールするコンポーネントが表示されます。[次へ] をクリックします。



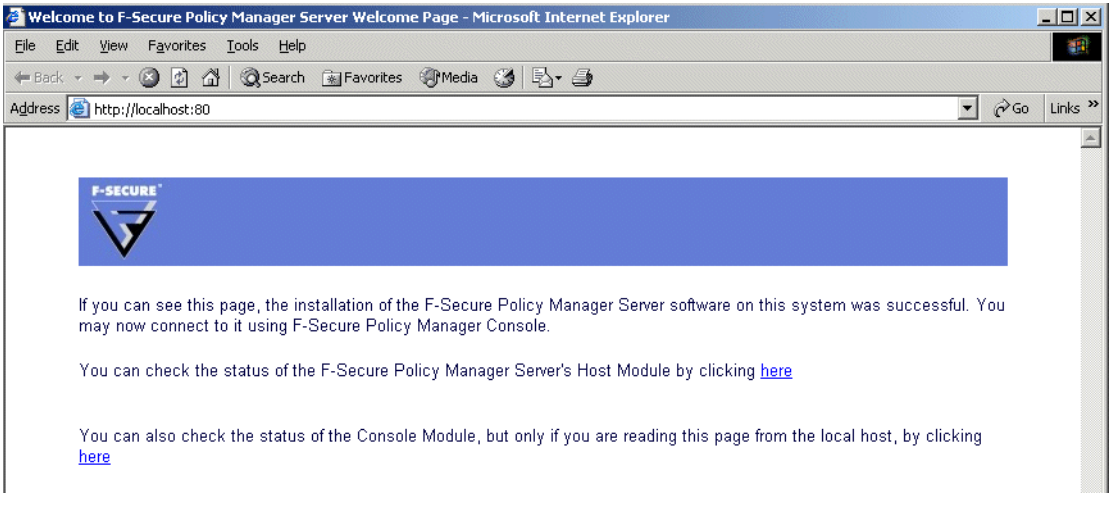
手順 12. セットアップが完了したら、すべてのコンポーネントが正常にインストールされたかどうかが表示されます。



手順 13. これで、F-Secure ポリシー マネージャ サーバがインストールされました。指示が表示された場合は、コンピュータを再起動します。[完了] をクリックしてインストールを完了します。



手順 14. インストールが正常に完了したかどうかを確認するために、F-Secure ポリシー マネージャ サーバをインストールしたコンピュータで Web ブラウザを開き、「http://localhost:80」と入力し（インストール時にデフォルトのポート番号を使用した場合）、ENTER キーを押します。サーバのインストールが正常に完了していれば、次のページが表示されます。



F-Secure ポリシー マネージャ サーバは、F-Secure ポリシー マネージャ コンソールによって通信ディレクトリが初期化された後でのみホストとして機能します。この初期化は、F-Secure ポリシー マネージャ コンソールを最初に起動したときに自動的に実行されます。

3.4 F-Secure ポリシー マネージャ サーバの設定

ポリシー マネージャ サーバのインストール先ディレクトリにある conf¥ ディレクトリに、httpd.conf という名前のファイルがあります。このファイルには、F-Secure ポリシー マネージャ サーバの設定情報が記述されています。

設定を変更した場合、変更を有効にするには、F-Secure ポリシー マネージャ サーバを停止して再起動する必要があります。

httpd.conf で設定できる F-Secure ポリシー マネージャ Web レポートの設定については、『Web レポートの管理』(P196) を参照してください。

3.4.1 通信ディレクトリのパスの変更

通信ディレクトリが配置されている既存のネットワーク ドライブがいっぱいになった場合、次の手順を使用して場所を変更することができます。

1. 空き領域の十分なドライブの新しいネットワーク パスを選択します。パスを作成し、fsms_<コンピュータの WINS 名> ユーザが、パス上のすべてのディレクトリに対してフル コントロールのアクセス権を持つことを確認します。
2. F-Secure ポリシー マネージャ サーバ サービスを停止します。
3. 古い commdir パスから、ディレクトリ全体を新しいパスにコピーします。
4. httpd.conf の `CommDir` と `CommDir2` ディレクティブの値を変更します。デフォルトでは次のような設定になっています。

   CommDir "C:¥Program Files¥F-Secure¥Management Server 5¥CommDir"

   CommDir2 "C:¥Program Files¥F-Secure¥Management Server 5¥CommDir"

   通信ディレクトリの場所を `E:\CommDir` に変更する場合は、次のようにディレクティブを変更してこの設定を反映させます。

   CommDir "E:¥CommDir"

   CommDir2 "E:¥CommDir"
5. F-Secure ポリシー マネージャ サーバのサービスを開始します。

6. すべてが正常に機能していることを確認します。
7. 古い commdir のファイルを削除します。

3.4.2 サーバが要求をリッスンするポートの変更

F-Secure ポリシー マネージャ サーバを構成する両方の WebServer モジュールのポートを定義するディレクティブには、Listen と <VirtualHost> の 2 つがあります。デフォルトでは、F-Secure ポリシー マネージャ サーバ管理モジュール（ポリシー マネージャ コンソールからの要求を処理するコンポーネント）はポート 8080 をリッスンし、F-Secure ポリシー マネージャ サーバ ホスト モジュール（ワークステーションからの要求を処理するコンポーネント）はポート 80 をリッスンします。ただし、デフォルトが適切ではない場合は、リッスンするポートを定義できます。

F-Secure ポリシー マネージャ サーバ管理モジュールがリッスンするポートを変更した場合は、環境設定ファイルに新しいポートを指定した Listen エントリ（例、Listen 8888）を追加し、F-Secure ポリシー マネージャ サーバ管理モジュールがリッスンするデフォルトのポートを定義している Listen ディレクティブ（Listen 8080）を削除します。

新しい Listen エントリを追加したら、古いエントリは必ず削除してください。古いエントリを削除しないと、サーバはネットワーク ポートなどのシステム リソースを不必要に消費します。

Listen ディレクティブを追加すると、F-Secure ポリシー マネージャ サーバは新しいポート（この例では 8888）をリッスンするよう認識します。ただし、F-Secure ポリシー マネージャ サーバ管理モジュールが新しいポートに関連付けられるよう設定する必要があります。この設定を行うには、<VirtualHost> ディレクティブを変更します。このディレ

クティブは F-Secure ポリシー マネージャ サーバ管理モジュールに関連付けられます。このディレクティブのデフォルト設定を次に示します。

```
#FSMSA port
<VirtualHost _default_:8080>
<Location /fsmsa/fsmsa.dll>
 SetHandler fsmsa-handler
</Location>
</VirtualHost>
```

新しく選択したポートに関連付けるには、このステートメントを次のように変更します。

```
#New FSMSA port
<VirtualHost _default_:8888>
<Location /fsmsa/fsmsa.dll>
 SetHandler fsmsa-handler
</Location>
</VirtualHost>
```

警告 ： ワークステーションが（F-Secure ポリシー マネージャ サーバ ホスト モジュールを経由して）にアクセスするように設定されている場合は、F-Secure ポリシー マネージャ サーバ ホスト ポートを変更しないでください。エージェントがこのポートを通信に使用しているため、ワークステーションがサーバに接続できなくなる場合があります。

3.4.3 F-Secure ポリシー マネージャ サーバの設定

ここでは、F-Secure ポリシー マネージャ サーバの環境設定ファイルにあるすべての関連エントリと、その使用方法について説明します。

ServerRoot ： このディレクティブは、サーバをインストールするディレクトリを設定します。他の環境設定ファイルの相対パスは、このディレクトリを基準にして設定されます。

Timeout : このディレクティブは、ネットワーク接続中に発信トラフィックも着信トラフィックもない場合に、サーバがセッションを閉じるまでの待機時間を定義します。

LoadModule : このディレクティブは、読み取るモジュールのシンボリック名と、モジュール バイナリが含まれるライブラリのパスを定義します。

例： `LoadModule fsmsh_module "C:\serverroot\modules\fsmsh.dll"`

Listen : このディレクティブは、サーバがリッスンするポートを定義します。たとえば、Web サーバのデフォルト設定は「`Listen 80`」などになります。接続の受信元を制限できます。たとえば、「`Listen 127.0.0.1:80`」と設定すると、サーバが実行されているコンピュータ（ローカルホスト）からポート 80 への接続のみが許可されます。

この設定および関連する `<VirtualHost>` 設定（この設定についてもここで説明します）を変更することにより、別のポートをリッスンするよう F-Secure ポリシー マネージャ サーバを設定できます。詳細については、『サーバが要求をリッスンするポートの変更』(P49) を参照してください。

DocumentRoot : このディレクティブでは絶対パスを使用する必要があります。このディレクティブは、すべてのユーザがアクセスできるディレクトリを定義するため、重要なデータが保存されているディレクトリのパスは使用しないでください。デフォルトで F-Secure ポリシー マネージャ サーバは、F-Secure ポリシー マネージャ サーバのインストール先ディレクトリにある `htdocs\` ディレクトリを割り当てます。このディレクトリには、サーバの初期画面が保存されています。このディレクトリのパスを変更すると、初期画面が表示されなくなります。

<ディレクトリ「c:¥パス名」>: このディレクティブは、パス部分で指定されたディレクトリに関連付けるセキュリティ設定を定義します。

ErrorLog : このディレクティブは、発生したエラーをサーバが記録するファイルの名前を設定します。ファイルのパスの先頭がスラッシュ (/) でない場合は、ServerRoot を基準とした相対パスとみなされます。ファイルのパスの先頭がパイプ (|) の場合は、エラー ログの処理を開始するためのコマンドとみなされます。この機能を使用して **rotatelog**

ユーティリティ（このセクションの **rotatelogs** エントリを参照）を起動すると、ログ ファイルを実際にローテーションさせて、書き込みによってファイルが無制限に増大するのを防ぐことができます。

<VirtualHost _default_:port> : このディレクティブは、仮想ホストにのみ適用されるディレクティブのセットを定義します。仮想ホストとは、仮想サーバ（他のサーバと同じプロセスで実行される別のサーバ）のことです。たとえば、F-Secure ポリシー マネージャ サーバには、ポート 80 で実行される仮想ホスト（F-Secure ポリシー マネージャ サーバ ホスト モジュール）と、ポート 8080 で実行される仮想ホスト（FSMSA または管理モジュール）の 2 つの仮想ホストがあります。

F-Secure ポリシー マネージャ サーバのデフォルト設定を示します。

```
# FSMSH port
<VirtualHost _default_:80>
<Location /fsms/fsmsh.dll>
SetHandler fsmsh-handler
</Location>
<Location /commdir>
SetHandler fsmsh-handler
</Location>
</VirtualHost>

#FSMSA port
<VirtualHost _default_:8080>
<Location /fsmsa/fsmsa.dll>
SetHandler fsmsa-handler
</Location>
</VirtualHost>
```

Commdir および **Commdir2** : これらのディレクティブは、通信ディレクトリまたはリポジトリのパスを定義します。このディレクトリには、F-Secure ポリシー マネージャ サーバがポリシー マネージャ コンソールと F-Secure 管理エージェントから受信するすべての管理データが保存されます。これらのディレクティブを変更して通信ディレクトリの場

所を変更できますが、サーバを実行するアカウント（fsms_<コンピュータの WINS 名>）が通信ディレクトリに対して完全な権限を持っていることを確認してください。

```
Commdir "C:\Program Files\F-Secure\Policy Manager
Server\CommDir"
Commdir2 "C:\Program Files\F-Secure\Policy Manager
Server\CommDir"
```

CustomLog ： このエントリは、サーバに対する要求をログに記録する場合に使用します。最初のパラメータには、ファイル（リクエストを記録するファイル）を指定するか、またはパイプ記号（|）の後に、標準入力上でログ情報を受信するプログラムのパスを指定します。この機能を使用して **rotatelog** ユーティリティ（このセクションの **rotatelogs** エントリを参照）を起動すると、ログ ファイルを実際にローテーションさせて、書き込みによってファイルが無制限に増大するのを防ぐことができます。

2 番目のパラメータには、ログ ファイルに書き込む内容を指定します。この内容は前の **LogFormat** ディレクティブで定義されています。

次に、access.log ファイルのエントリの例を示します。

```
10.128.131.224 - - [18/Apr/2002:14:06:36 +0300]
/fsmsa/fsmsa.dll?FSMSCommand=ReadPackage&Type=27&SessionID=248 HTTP/1.1"
200 5299 0 - 0 - "FSA/5.10.2211 1.3.1_02 Windows2000/5.0 x86"
mod_gzip:DECHUNK:DECLINED:TOO_SMALL CR:0pct.
```

「10.128.131.224 - - [18/Apr/2002:14:06:36 +0300]」は、サーバへの要求がいつどのホストによって行われたかを表します（ホストは IP アドレスで表されます）。

コマンドがどのモジュールを /fsmsa/fsmsa.dll に送信したかは、fxnext コンポーネントによって通知されます。このモジュール（fsmsa.dll）は管理モジュールです。fsmsh.dll はホスト モジュールです。

その後に、FSMSCommand=ReadPackage&Type=27&SessionID=248 というコマンドとパラメータが続きます。この場合、ホストはタイプ 27 のオブジェクト（1 つしか存在しません）を要求しています。

使用されている HTTP のバージョンも HTTP/1.1 と記録されています。

HTTP バージョンのすぐ後には、異なる 6 つの数字が続きます。各数字の意味は次のとおりです。

1. HTTP 応答コード： この例では、200 が使用されています（HTTP 仕様で「OK」を表します）。他にもコードがあり、コードはすべて HTTP 仕様に基づいています。HTTP 仕様については、http://www.w3.org を参照してください。
2. サーバから転送されたバイト数 ： このエントリの例では 5299 バイトが転送されています。
3. サーバが要求に応答するまでの所要時間（秒単位）。
4. 応答が完了した時点での接続ステータス。
   「X」： 応答が完了する前に接続が中止されました。
   「+」： 応答送信後も接続を維持できます。
   「-」： 応答送信後に接続が終了します。
5. F-Secure ポリシー マネージャ サーバ管理モジュールのエラーコード（成功した場合は 0）。
6. サーバに転送されたバイト数（ない場合は「-」）。

次の文字列「FSA/5.10.2211 1.3.1_02 Windows2000/5.0 x86」は、クライアントを識別します。この場合、FSA 5.10 ビルド 2211 がサーバにアクセスしました。

この後に続く「mod_gzip: DECHUNK:DECLINED:TOO_SMALL」は、データの圧縮に関する情報です。
この例では、データは小さすぎるため圧縮されていません。

最後の「CR:0pct」は圧縮率を表します。この例では 0% です。

Rotatelogs: F-Secure ポリシー マネージャ サーバが生成するログをローテーションするために使用される小規模なプログラムです。これを使用して、ログの保存期間（デフォルトでは 8 日間）と、ファイルをローテーションする周期を定義できます。たとえば、access.log のファイル名を access.log.1 に変更したときに、新しい空の access.log を作成し、このファイルに新しい要求を記録します。

次に使用例を示します。

```
CustomLog '|""C:\Program Files\F-Secure\Policy Manager Server
5\bin\rotatelogs"
"C:\Program Files\F-Secure\Policy Manager Server
5\logs\access.log" 8 86400"' common"
```

この例では、RotateLogs ユーティリティで access.log ファイルを開き、8 つのファイル（現在使用中のファイルと 8 つのアーカイブ ファイル）を毎日（86400 秒 = 24 時間）ローテーションするように CustomLog ディレクティブを定義しています。つまり、過去 1 週間と 1 日分のファイルが保持され、さらに当日のアクセスを記録するファイルがあることになります。

<ifModule mod_gzip.c> : F-Secure ポリシー マネージャ サーバには、コンソールとサーバの間で転送されるすべてのデータを圧縮できる新しい機能があります。このディレクティブは圧縮設定の開始位置を示し、</ifModule> ディレクティブの直前で終了します。圧縮設定の詳細については、httpd.sample ファイルを参照してください。このファイルは、F-Secure ポリシー マネージャ サーバの環境設定ファイルと同じディレクトリ（<F-Secure ポリシー マネージャ サーバのインストール先ディレクトリ >¥conf）にあります。

mod_gzip_on Yes : この設定は圧縮設定の 1 つで、F-Secure ポリシー マネージャ サーバの圧縮サポートを有効または無効にします。この設定を mod_gzip_on No に変更すると、圧縮は無効になります。

FastPolicyDistribution On : これは、パフォーマンスと最大限の下位互換性を切り替えるスイッチです。有効（On）にした場合、F-Secure ポリシー マネージャ サーバは非常に高速にポリシーを配布できます（30 ～ 100 倍。ホストの数により異なる）。他のコンポーネント（F-Secure 管理エージェントなど）が通信ディレクトリに同時にアクセスする場合は、無効化スイッチ（Off）を使用してください。

RetryFileOperation 10 : ファイル操作が失敗した場合、失敗した操作を中止するまでに（1 秒の間隔で）再試行する回数を設定します。

CommdirCacheSize 10 : この設定の数値は、提供前のファイルをあらかじめメモリに格納しておくために使用するメモリの量（パーセント単位）をサーバに通知します。これにより、常にディスクからファイルを読み取らなくてもよくなるため、サーバはファイルを迅速に提供できるよ

うになります。デフォルト（10）を使用すると、サーバはメモリの 10% をこのキャッシュのために使用します。たとえば、512MB の RAM を搭載したマシンでは、51.2MB がキャッシュに使用されます。

3.5 F-Secure ポリシー マネージャ サーバのアンインストール

F-Secure ポリシー マネージャ サーバ（または、その他の F-Secure ポリシー マネージャ コンポーネント）をアンインストールするには、以下の手順を実行します。

1. Windows の［スタート］メニューを開き、［コントロール パネル］を選択します。［プログラムの追加と削除］を選択します。
2. F-Secure ポリシー マネージャ サーバ（またはアンインストールするコンポーネント）を選択して、［**追加と削除**］ボタンをクリックします。
3. ［F-Secure のアンインストール］ダイアログ ボックスが表示されます。［**開始**］をクリックしてアンインストールを開始します。
4. アンインストールが終了したら、［**閉じる**］をクリックします。
5. ［OK］をクリックして、［プログラムの追加と削除］を終了します。
6. 変更を有効にするために、コンピュータを再起動します。

4 通信ディレクトリの移行

はじめに 58
移行の手順 58

4.1 はじめに

F-Secure ポリシー マネージャ 6.0 より以前のバージョンでは F-Secure ポリシー マネージャ サーバの代わりに通信ディレクトリ (CommDir) を使用することができましたが、バージョン 6.0 以降からは通信ディレクトリはサポートされていません。これによって、既存の CommDir ベースのインストールがある場合は、F-Secure ポリシー マネージャ サーバのインストールにアップグレードする必要があります。

この章では 既存システムのバックアップからネットワーク内のホストが F-Secure ポリシー マネージャ サーバ と正常に通信するまでの手順を含めた、CommDir ベースのインストールからポリシー マネージャ サーバへの移行を説明します。

4.2 移行の手順

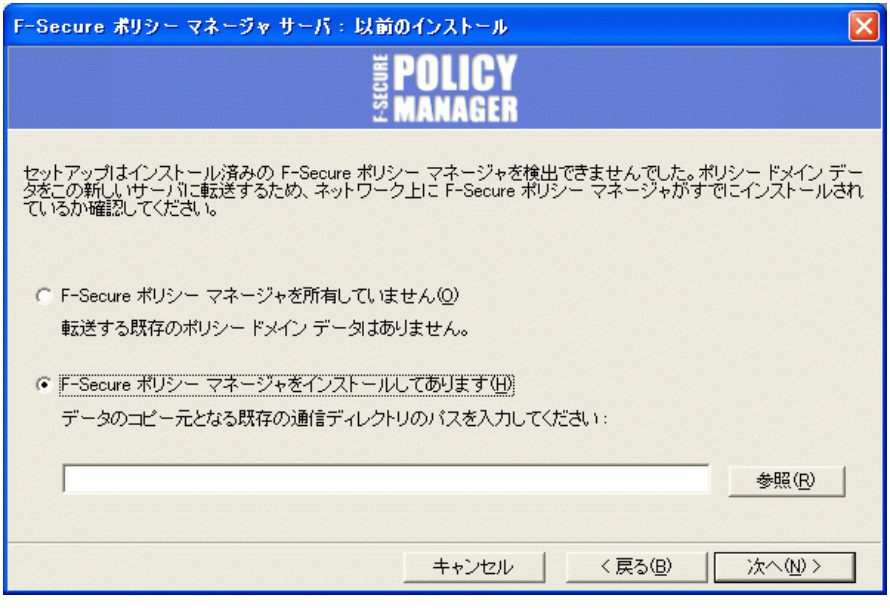
CommDir のインストールからポリシー マネージャ サーバのインストールに移行するには、次の手順を実行します。

手順 1. 既存のシステムをバックアップする

1. バックアップを始める前に、F-Secure ポリシー マネージャ コンソール が起動していないことを確認します。
2. 管理用鍵 (admin.pub および admin.prv) と既存の CommDir をバックアップします。デフォルトで管理用鍵は C:¥Program Files¥F-Secure¥Administrator¥ に保存されています。

手順 2. 新しい F-Secure ポリシー マネージャ サーバ とコンソールをインストールする

1. 新しい F-Secure ポリシー マネージャ サーバ とコンソールをインストールします。手順については、『F-Secure ポリシー マネージャ サーバのインストール』(P25) および『F-Secure ポリシー マネージャ コンソールのインストール』(P63) を参照してください。
2. F-Secure ポリシー マネージャ サーバのインストール中に、既存の CommDir データを手順 1 で作成したバックアップからコピーします。下図のダイアログが表示したら、［参照 ...］をクリックして、バックアップを指定します。



3. バックアップを指定したら、確認のダイアログが表示されます。[OK] をクリックして続行します。

手順 3. ポリシー マネージャ コンソールを新しいポリシー マネージャ サーバに接続する

1. F-Secure ポリシー マネージャ コンソールを新しい F-Secure ポリシー マネージャ サーバ に接続します。
2. F-Secure ポリシー マネージャ サーバのアドレスを指定します。
   - ［設定］タブを選択して、［集中管理］ページを開きます。
   - F-Secure ポリシー マネージャ サーバのアドレスを http://<IP address> の形式で入力します。
3. 管理ドメイン全体にポリシーを配布します。
4. F-Secure ポリシー マネージャ コンソールを終了します。

手順 4. 以前の CommDir に接続を設定する

1. F-Secure ポリシー マネージャ コンソールを以前の Commdir に接続します。
2. F-Secure ポリシー マネージャ サーバのアドレスを指定します。
   - ［設定］タブを選択して、［集中管理］ページを開きます。
   - F-Secure ポリシー マネージャ サーバのアドレスを http://<IP address> の形式で入力します。
3. 管理ドメイン全体にポリシーを配布します。
4. F-Secure ポリシー マネージャ コンソールを終了します。

手順 5. 移行が完了するのを待つ

すべてのホストが以前の CommDir ではなく、新しい F-Secure ポリシー マネージャ サーバと通信していることを確認します。ホストの数によって、すべて確認するのに一週間以上かかることがあります。

F-Secure ポリシー マネージャ コンソールの［サマリ］タブから通信状況を確認できます。［最新ポリシーを持つホストの割合］が 100% になった時点で、移行は完了です。

5 F-SECURE ポリシー マネージャ コンソールのインストール

概要 64
インストールの手順 64
F-Secure ポリシー マネージャ コンソールのアンインストール 82

5.1 概要

F-Secure ポリシー マネージャ コンソールは用途別に、2 つのモードをご利用できます。

- 管理者モード ： F-Secure ポリシー マネージャ コンソールを全範囲で使用できます。
- 読み取り専用モード ： F-Secure ポリシー マネージャ コンソールの情報を表示できますが、管理タスクは実行できません（このモードはヘルプデスク スタッフなどのユーザに便利です）。

コンソールをインストールしたら、管理者モードと読み込み専用モードを両方使用できます。次の章では、F-Secure CD から F-Secure ポリシー マネージャ コンソールのセットアップを実行する方法と、初めてコンソールを実行するときに初期操作モードを選択する方法について説明します。CD によるセットアップ方法はどちらのモードの場合でも同じです。また、新しい管理者および読み取り専用の接続は、初めて起動した後にいつでも追加することができます。

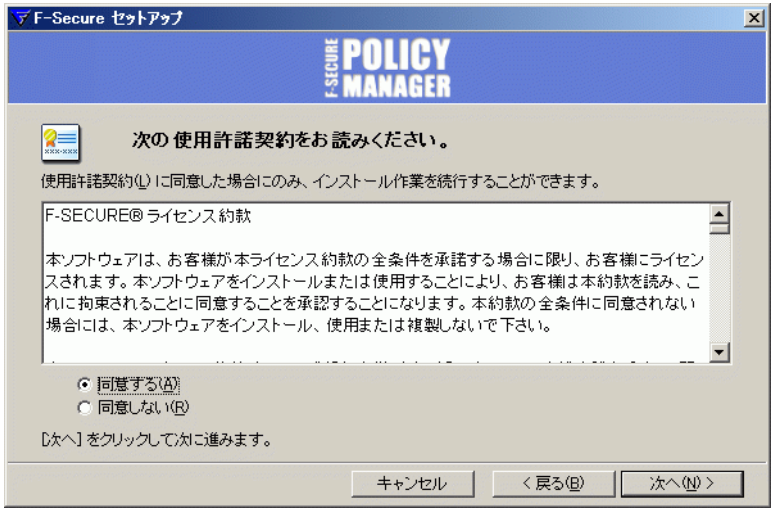
5.2 インストールの手順

手順 1.

1. F-Secure CD を CD-ROM ドライブに挿入します。
2. ［企業用］を選択します。［次へ］をクリックして続行します。
3. ［管理ソフトウェアのインストールまたは更新］メニューから、[F-Secure ポリシー マネージャ］を選択します。

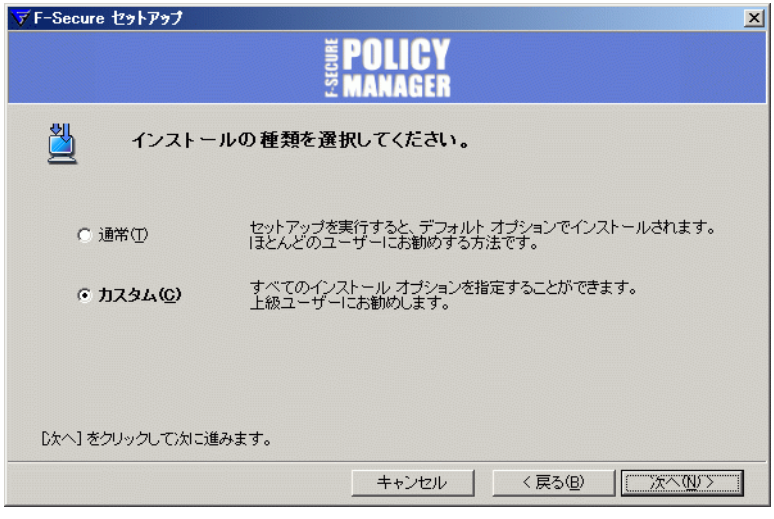
手順 2. ようこその画面が表示されたら、セットアップ画面の指示に従います。ドロップダウン メニューからインストール言語を選択します。[次へ] をクリックして続行します。

手順 3. 使用許諾契約の情報を読みます。同意する場合は、[同意する] を選択します。[次へ] をクリックして続行します。



手順 4. インストールの種類を選択します。

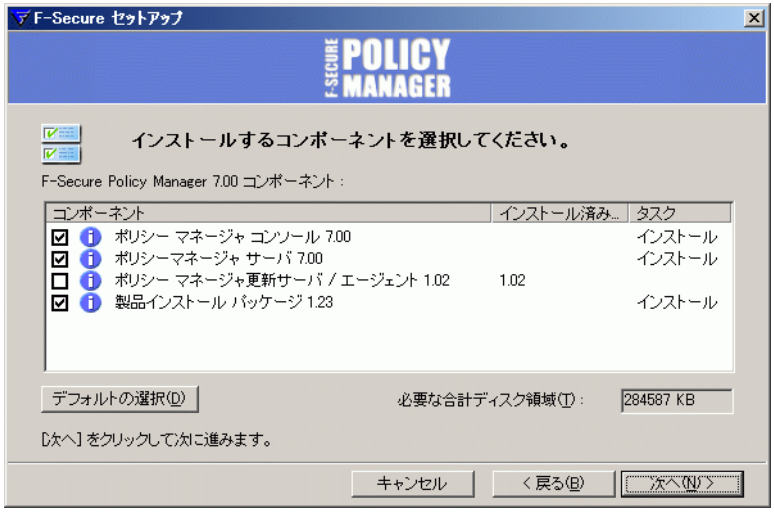
- **通常**
  製品をデフォルトのオプションでインストールします。
  - F-Secure ポリシー マネージャ サーバ、F-Secure ポリシー マネージャ コンソール、F-Secure ポリシー マネージャ更新サーバおよびエージェントが同じコンピュータにインストールされます。
  - デフォルトのポートは F-Secure ポリシー マネージャ サーバ モジュールによって使用されます。
  - 同じコンピュータにインストールされた F-Secure ポリシー マネージャ コンソールのみが、F-Secure ポリシー マネージャ サーバにアクセスできます。
  - Web レポートへのアクセスは、他のコンピュータからも許可されます。
- **カスタム**
  インストール先ディレクトリや F-Secure ポリシー マネージャ サーバ モジュールが使用するポートなどを指定できます。一部のダイアログは、[カスタム] を選択した場合にのみ表示されます。
- **再インストール**
  既存のコンポーネントをすべて再インストールし、不足している設定を復元します。このオプションは、コンピュータに F-Secure ポリシー マネージャがインストールされている場合にのみ表示されます。


F-Secure セットアップ
F-SECURE POLICY MANAGER
インストールの種類を選択してください。
通常(T)
セットアップを実行すると、デフォルト オプションでインストールされます。
ほとんどのユーザーにお勧めする方法です。
カスタム(C)
すべてのインストール オプションを指定することができます。
上級ユーザーにお勧めします。
[次へ] をクリックして次に進みます。
キャンセル
< 戻る(B)
次へ(N) >

手順 5. 次のコンポーネントをインストールするように選択します。

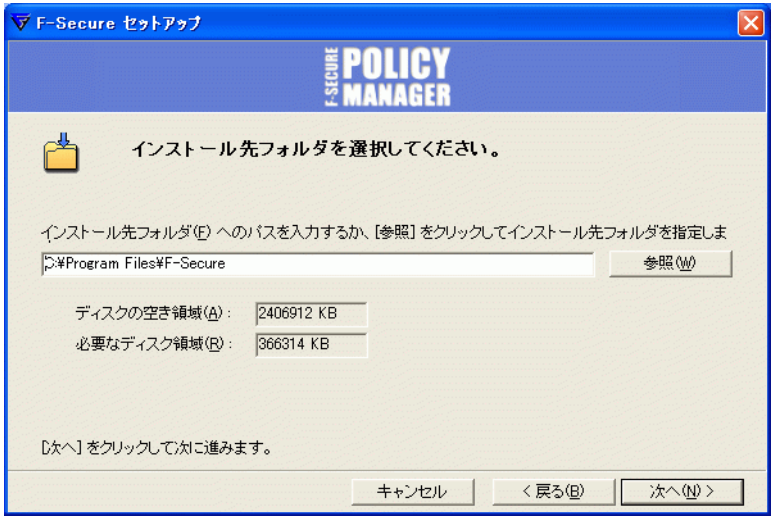
- F-Secure ポリシー マネージャ コンソール
- F-Secure VPN+ 認証ウィザード（オプション。F-Secure VPN+ 管理にのみ必要）

［次へ］をクリックして続行します。

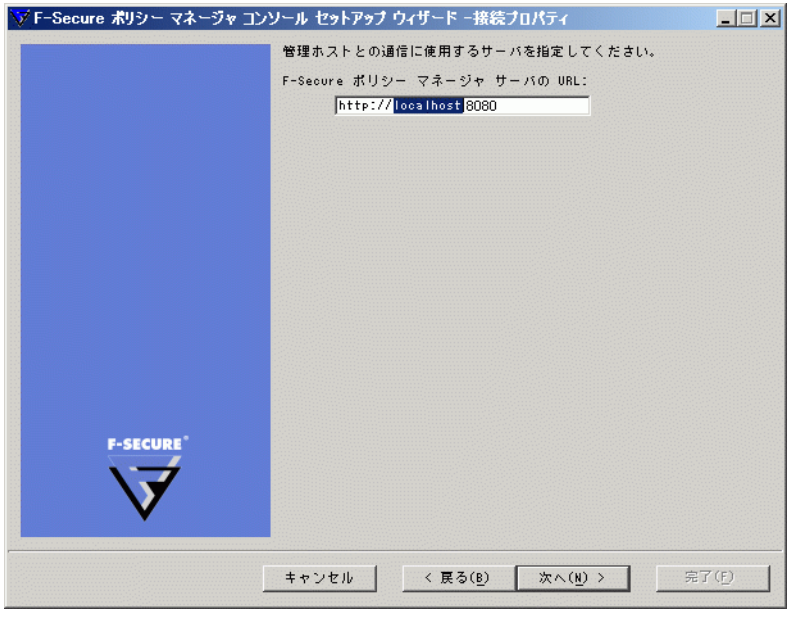


手順 6. インストール先フォルダを選択します。［次へ］をクリックします。

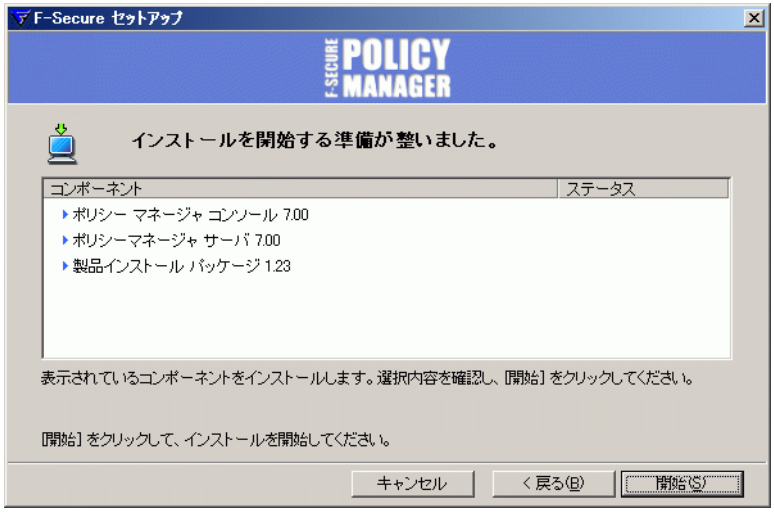
デフォルトのインストール先ディレクトリを使用することを推奨します。F-Secure ポリシー マネージャ コンソールを別のディレクトリにインストールするには、［参照］ をクリックします。



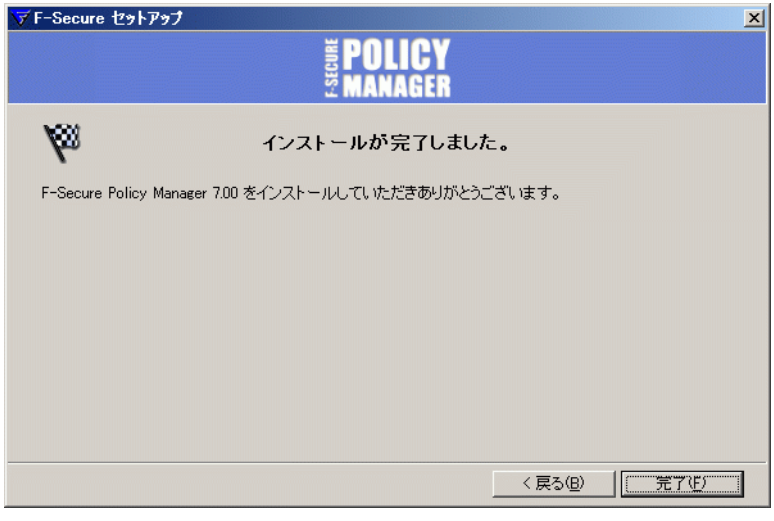
手順 7. F-Secure ポリシー マネージャ サーバのアドレスと管理ポート番号を指定します。［次へ］をクリックして続行します。



手順 8. セットアップが行う変更を確認します。［次へ］をクリックして続行します。



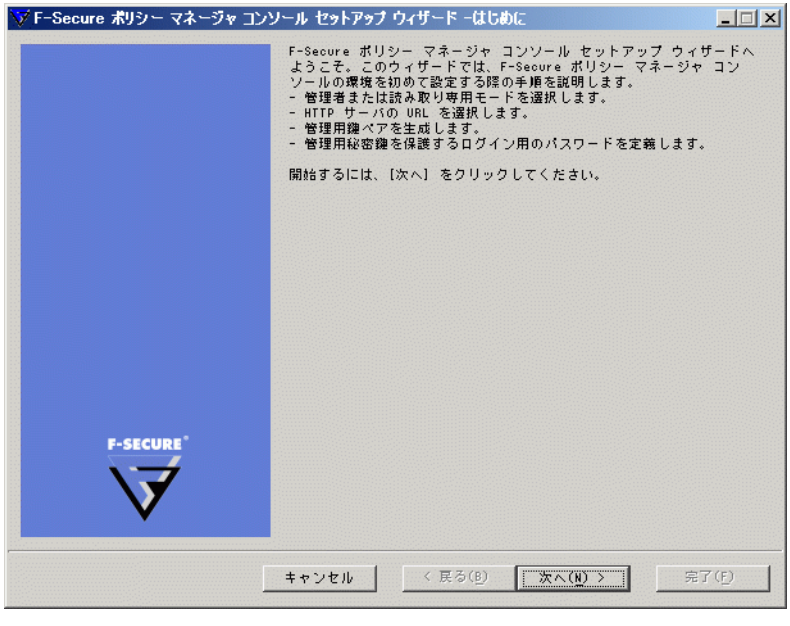
手順 9. デフォルトでは、CD セットアップが実行された直後に F-Secure ポリシー マネージャ コンソールが実行されます。一部の接続プロパティはコンソールを初めて起動したときに収集されるため、セットアップ後にコンソールを実行することは重要です。［完了］をクリックして、F-Secure ポリシー マネージャ コンソールを起動します。



手順 10.

セットアップ完了直後に F-Secure ポリシー マネージャ コンソールを起動するように選択しない場合は、[スタート] -> [プログラム] -> [F-Secure ポリシー マネージャ コンソール] -> [F-Secure ポリシー マネージャ コンソール] のショートカットから起動することができます。F-Secure ポリシー マネージャ コンソールを初めて実行するときには、コンソール セットアップ ウィザードがサーバへの初期接続を作成するために必要な情報を収集します。通常、この手順は手順 1 ～ 8 で説明された F-Secure CD からのコンソールのインストール直後に実行されます。

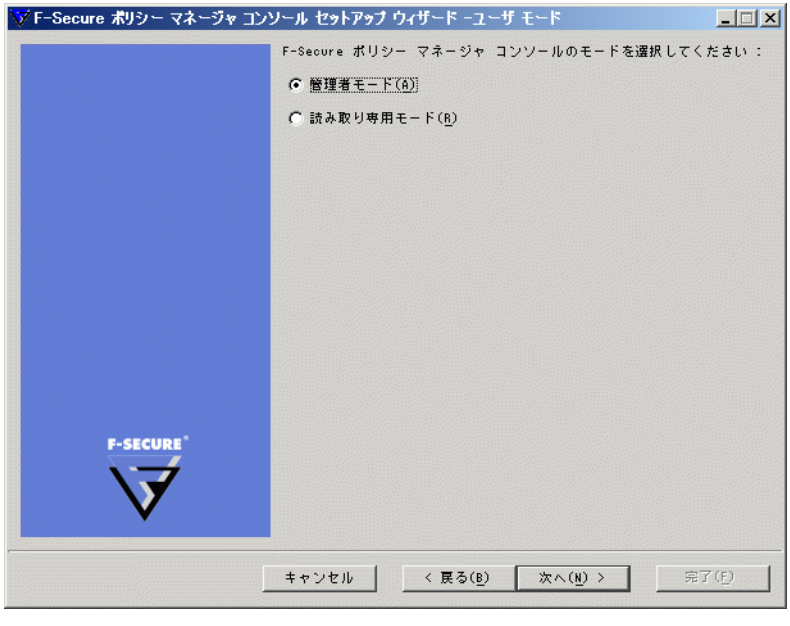
F-Secure ポリシー マネージャ コンソールのセットアップ ウィザードの最初のページには、インストールの概要が表示されます。[次へ] をクリックして続行します。



手順 11. 必要に応じたユーザ モードを選択します。

- **管理者モード**
  管理者の機能をすべて有効にします。
- **読み取り専用モード**
  管理者のデータを表示できますが、変更は行えません。[読み取り専用モード] を選択した場合、ホストを管理することはできません。管理者モードに変更するには、管理用鍵の admin.pub および admin.prv が必要となります。

[次へ] をクリックして続行します。

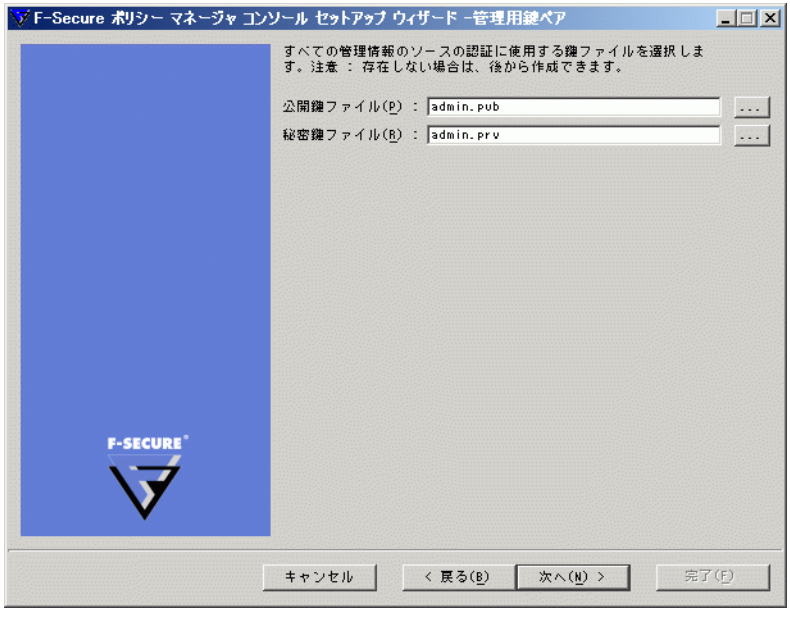


手順 12. 管理者の公開鍵ファイルと秘密鍵ファイルを格納する場所のパスを入力します。デフォルトでは、鍵ファイルは以下の F-Secure ポリシー マネージャ コンソールのインストール ディレクトリに格納されます。

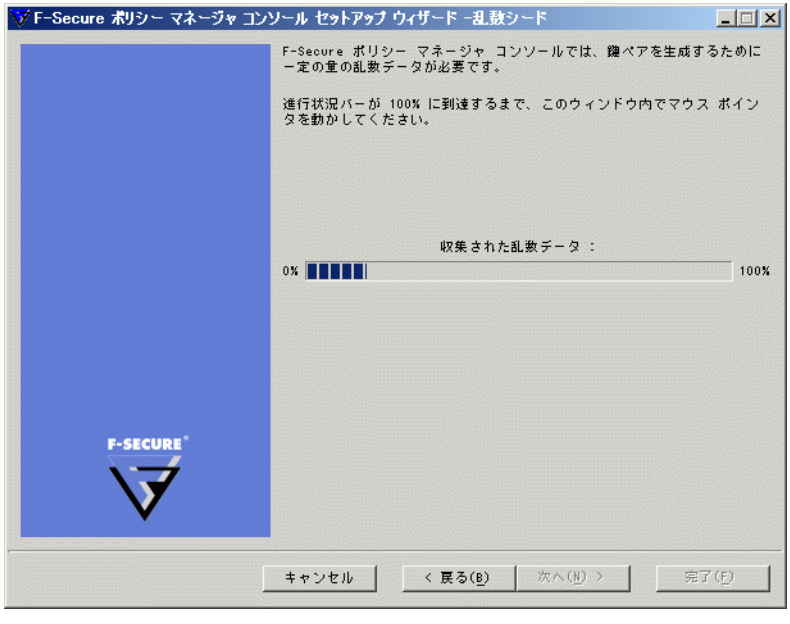
Program Files¥F-Secure¥Administrator

［次へ］をクリックして続行します。

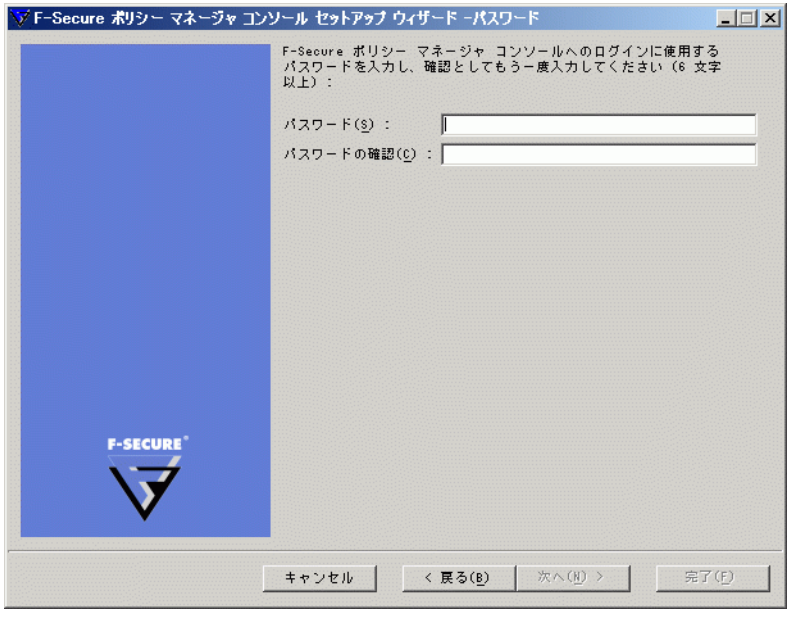
鍵ペアがすでに存在しない場合、鍵ペアはセットアップの後半で作成されます。



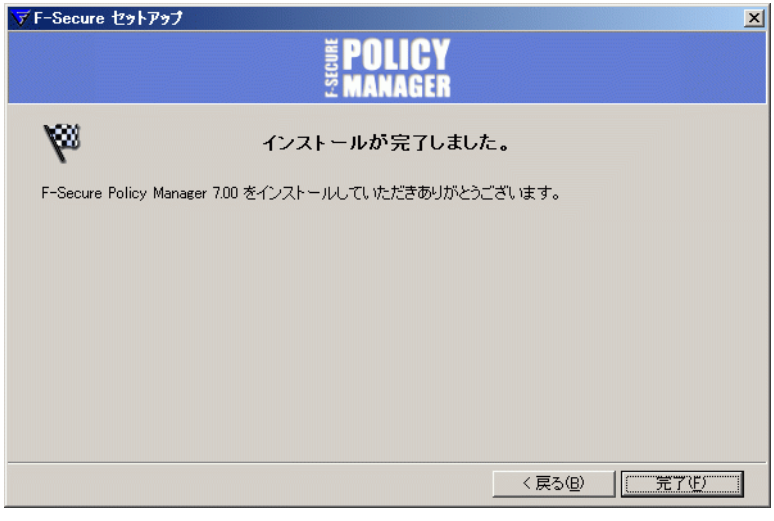
手順 13. マウスのカーソルをウィンドウ内で動かして、管理用鍵ペア ジェネレータで使用する乱数シードを初期化します。マウスを動かした曲線を使用することにより、鍵ペア生成アルゴリズムのシード値は十分な乱数を得ることができます。進行状況を示すインジケータが 100% になると、［パスワード］ダイアログ ボックスが自動的に開きます。



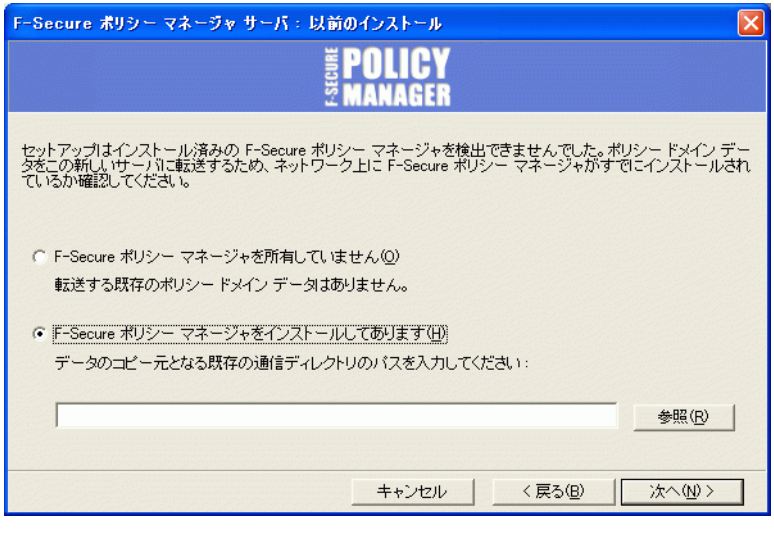
手順 14. 管理用秘密鍵を保護するパスワードを入力します。[パスワードの確認] フィールドに、パスワードを再入力します。[次へ] をクリックします。



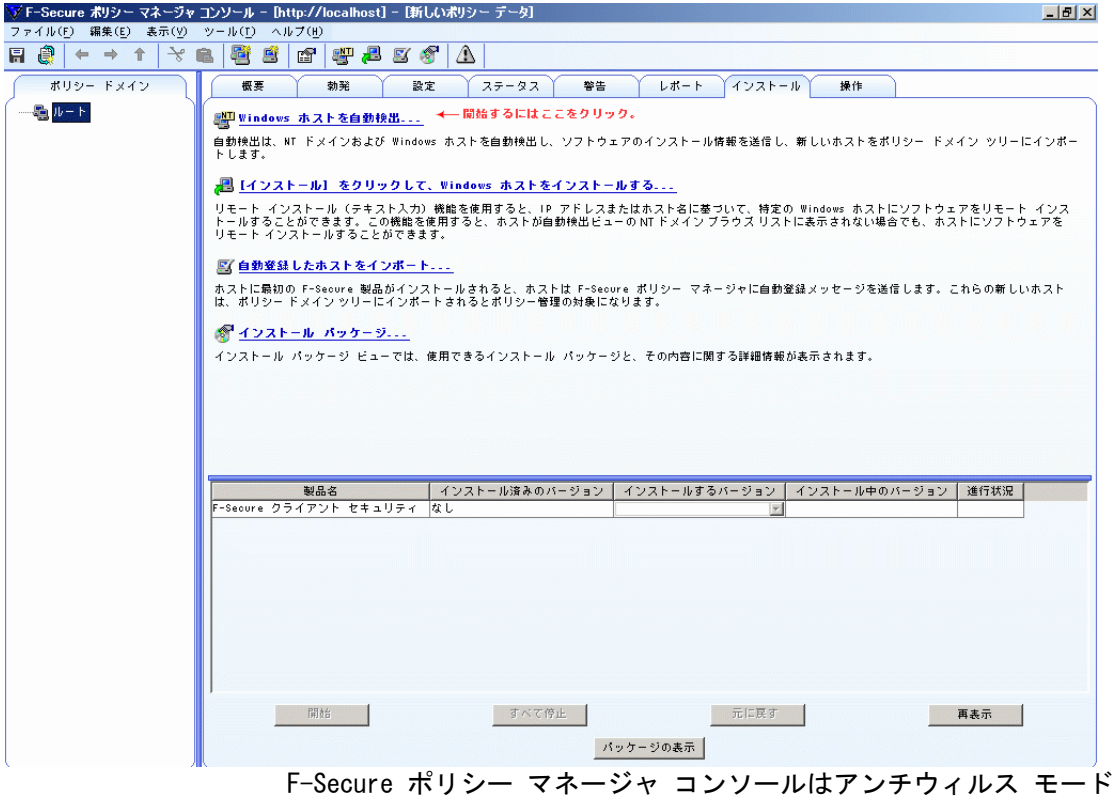
手順 15. [完了] をクリックして、セットアップを完了します。



F-Secure ポリシー マネージャ コンソールは管理用の鍵ペアを生成します。



鍵ペアが生成されると、F-Secure ポリシー マネージャ コンソールが起動します。



F-Secure ポリシー マネージャ コンソールはアンチウィルス モードで起動します。このモードは、F-Secure クライアント セキュリティおよび F-Secure アンチウィルス ワークステーション版を管理するために最適化されたユーザ インタフェースです。F-Secure ポリシー マネージャ コンソールを使用して他の F-Secure 製品を管理する場合は、詳細モードのユーザ インタフェースを使用する必要があります。詳細モードのユーザ インタフェースに切り替えるには、[表示] メニューを開いて [詳細モード] を選択します。

ワークステーションをセットアップする場合、Admin.pub 鍵ファイルのコピーを送信（またはそこにアクセス）する必要があります。F-Secure ポリシー マネージャを使用して F-Secure 製品をリモートでワークス

テーションにインストールすると、Admin.pub 鍵ファイルのコピーが自動的にワークステーションにインストールされます。ただし、CD からセットアップを実行した場合は、Admin.pub 鍵ファイルのコピーを手動でワークステーションに転送する必要があります。最も安全な方法は、Admin.pub ファイルをフロッピー ディスクにコピーし、そのフロッピー ディスクを使用してワークステーションにインストールを行う方法です。または、リモート管理の F-Secure 製品でインストールされるホストすべてがアクセスできるディレクトリに、Admin.pub ファイルを格納することもできます。デフォルトでは、F-Secure ポリシー マネージャ コンソールは公開鍵を通信ディレクトリのルートに格納します。

一部のディレクトリやファイルは、管理者のみがアクセスできるようにアクセス権を設定して保護する必要があります。アクセス権を設定するには、次の手順に従います。

1. ¥fsa サブディレクトリに対する不要なアクセス権をすべて削除します。F-Secure ポリシー マネージャ コンソールを実行する管理者のみが、このディレクトリに対するアクセス権を持つように設定します。
2. commdir.cfg と admin.pub から不要な書き込み / 変更アクセス権を取り外します。通信ディレクトリには、これらのファイルに対する読み取り専用権限を設定します。

インストールが完了すると、F-Secure ポリシー マネージャが起動します。この時点で、ポリシー ドメインを作成してホストをインストールすることができます。

Web ブラウザのパスの変更

F-Secure ポリシー マネージャ コンソールは、セットアップ中にデフォルトの Web ブラウザへのファイル パスを取得します。Web ブラウザのパスを変更する場合は、[ツール] メニューを開き、[一般設定] を選択します。

[場所] タブを選択して、新しいファイル パスを入力します。

5.3 F-Secure ポリシー マネージャ コンソールのアンインストール

F-Secure ポリシー マネージャ コンソール（またはその他の F-Secure ポリシー マネージャ コンポーネント）をアンインストールするには、以下の手順を実行します。

1. Windows の［スタート］メニューを開き、［コントロール パネル］を選択します。［アプリケーションの追加と削除］を選択します。
2. アンインストールするコンポーネント（F-Secure ポリシー マネージャ コンソールまたは認証ウィザード）を選択して、**［追加と削除］**をクリックします。
3. [F-Secure のアンインストール］ダイアログ ボックスが表示されます。**［開始］**をクリックしてアンインストールを開始します。
4. アンインストールが完了したら、**［閉じる］**をクリックします。
5. [OK] をクリックして、［アプリケーションの追加と削除］を終了します。
6. 変更を有効にするために、コンピュータを再起動します。

6 F-SECURE ポリシー マネージャ コンソールの使用

概要 84
F-Secure ポリシー マネージャ コンソールの基本機能 85
F-Secure クライアント セキュリティの管理 ... 103
ドメインとホストの管理 104
ソフトウェアの配布 115
ポリシーの管理 134
操作とタスクの管理 140
警告の送信 141
レポート ツール 143
一般設定 148

6.1 概要

F-Secure ポリシー マネージャ コンソールは、F-Secure の主要なセキュリティ製品をリモート管理するためのコンソールで、企業ネットワークに必要なすべてのセキュリティ管理機能の共通プラットフォームを備えています。

管理者は、ホストごとに異なるセキュリティ ポリシーを作成でき、複数のホスト用に 1 つのポリシーを作成することもできます。ポリシーはネットワークを通じてワークステーション、サーバ、およびセキュリティ ゲートウェイに配布できます。

F-Secure ポリシー マネージャ コンソールでは、以下の操作を実行できます。

- 管理対象製品の属性値の設定
- 管理者がリモート操作で設定した属性値を、ユーザが表示または変更できるように権限を決定
- 共通の属性値を持つ管理対象ホストを特定のポリシー ドメインでグループ化
- ホストとドメイン階層の容易な管理
- 属性値や制約など、署名されたポリシー定義の生成
- ステータス表示
- 警告の処理
- F-Secure アンチウィルスのスキャン レポートの処理
- リモート インストールの処理
- HTML 形式でのレポートの表示、またはさまざまなエキスポート形式へのレポートの変換

F-Secure ポリシー マネージャ コンソールはポリシー定義を生成し、ステータスおよび警告を表示します。各管理対象ホストに、ホストに対してポリシーを実施するためのモジュール（F-Secure 管理エージェント）があります。

F-Secure ポリシー マネージャ コンソールでは、複数のホストをポリシー ドメイン内でグループ化して管理します。ポリシーはホスト単位で指定します。マルチユーザ環境でも、特定のホストに含まれる全ユーザが同じ設定を共有します。

F-Secure ポリシー マネージャ コンソールには、管理者と読み取り専用モード ユーザの 2 種類のユーザが存在します。

管理者は、管理用秘密鍵へアクセスできます。秘密鍵はファイルとして保存されており、管理権を所有するユーザ間でこの鍵を共有することができます。管理者は F-Secure ポリシー マネージャ コンソールを使用して、各ドメインおよび個々のホストに対してポリシーを定義します。

読み取り専用モードでは、ユーザは次の操作を行うことができます。

- ポリシー、統計情報、操作ステータス、インストールされている製品のバージョン番号、警告、およびレポートの表示
- F-Secure ポリシー マネージャ コンソールのプロパティの変更（ユーザ単位でインストールされるので、変更は他のユーザには影響しません）

読み取り専用モードでは、次のタスクは実行できません。

- ドメイン構造や、ドメインおよびホストのプロパティの変更
- 製品の設定の変更
- 操作の実行
- 製品のインストール
- ポリシー データの保存
- ポリシーの配布
- 警告やレポートの削除

F-Secure ポリシー マネージャ サーバへの管理者モード接続は、一度に 1 つだけ許可されます。F-Secure ポリシー マネージャ サーバへの読み取り専用接続は、一度に複数の接続が可能です。

6.2 F-Secure ポリシー マネージャ コンソールの基本機能

この後の各セクションでは、F-Secure ポリシー マネージャ コンソールのログオン手順、メニュー コマンド、基本操作について説明します。

6.2.1 ログイン

F-Secure ポリシー マネージャ コンソールを起動すると、次のダイアログ ボックスが表示されます（[**オプション**] をクリックするとダイアログ ボックスが拡大表示され、他のオプションが表示されます）。

図 6-1 F-Secure ポリシー マネージャ コンソールのログイン ダイアログ

ダイアログ ボックスを使用して、定義済みの接続を選択できます。各接続は個別の設定を持つため、F-Secure ポリシー マネージャ コンソールの 1 つのインスタンスで複数のサーバを簡単に管理できます。

また、1 台のサーバに複数の接続を定義することもできます。接続を選択したら、F-Secure ポリシー マネージャ コンソールのパスワードを入力します。プログラムのインストール時に定義したパスワードを入力します。このパスワードは、ネットワーク管理者のパスワードではありません。

パスワードを入力する必要がない場合は、読み取り専用モードでプログラムを起動できます。ただし、この場合に変更を加えることはできません。

セットアップ ウィザードにより初期接続が作成され、接続情報がデフォルトで［接続］フィールドに表示されます。さらに接続を追加する場合は［ **追加** ］をクリックします。既存の接続を編集する場合は［ **編集** ］をクリックします（これらのオプションはダイアログ ボックスが拡大表示されているときに使用できます）。

既存の接続のコピーを作成することができます。これにより、さまざまな使用方法でわずかに異なる接続設定を使用して、同じサーバに複数の接続を簡単に定義できます。例えば、既存の接続をテンプレートとすると、元の設定に影響を与えることなく、異なる接続設定を新しいコピーでテストできます。

接続プロパティ

データ リポジトリへのリンクは、F-Secure ポリシー マネージャ サーバの HTTP URL として定義します。

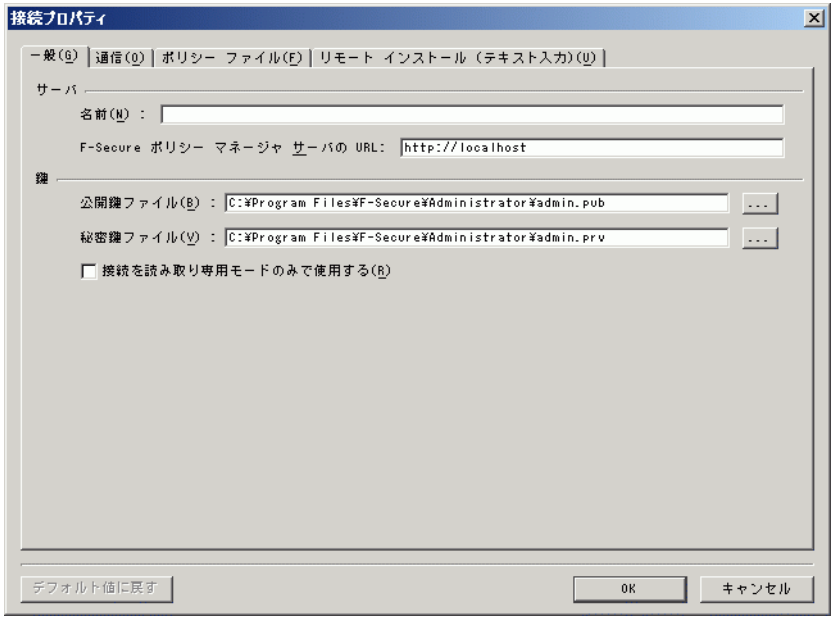


図 6-2［接続プロパティ］ダイアログ

［名前］フィールドには、ログイン ダイアログの［接続］フィールドに表示される接続名を指定します。［名前］フィールドを空のままにしておくと、URL またはディレクトリ パスが表示されます。

［公開鍵ファイル］および［秘密鍵ファイル］フィールドには、この接続で使用する管理用鍵ペアを指定します。指定した鍵ファイルが存在しない場合、F-Secure ポリシー マネージャ コンソールは新しい鍵ペアを生成します。

通信の一般設定

通信設定をカスタマイズするには、［通信］タブを選択します。［**ポーリング間隔のオプション**］をクリックすると、ポーリング間隔を変更できます。

［ホストの接続ステータス］には、ホストが F-Secure ポリシー マネージャから切断されたと見なされる時間を設定します。定義した時間内に F-Secure ポリシー マネージャ サーバと通信しなかったホストは、すべて切断したものと見なされます。切断されたホストのドメイン ツリーには通知アイコンが表示されます。さらに、これらのホストは［ドメインのステータス］ビューの［接続を切断されたホスト］リストに表示されます。ドメイン ツリーに通知アイコンを表示するかどうかは、［**詳細オプション**］で切り替えることができます。間隔が 1 日未満の場合は、設定フィールドに浮動少数点数で入力することにより簡単に定義できます。例えば値が「0.5」の場合、12 時間以内にサーバに接続しなかったホストはすべて切断されたものとみなされます。通常、1 日未満の値はトラブルシューティングの場合に便利です。通常の環境でも、ホストによってはときどきサーバから切断されるのが自然な動作であるためです。たとえば、ノート型コンピュータはサーバに毎日アクセスできない可能性がありますが、通常はこれは正常な現象です。

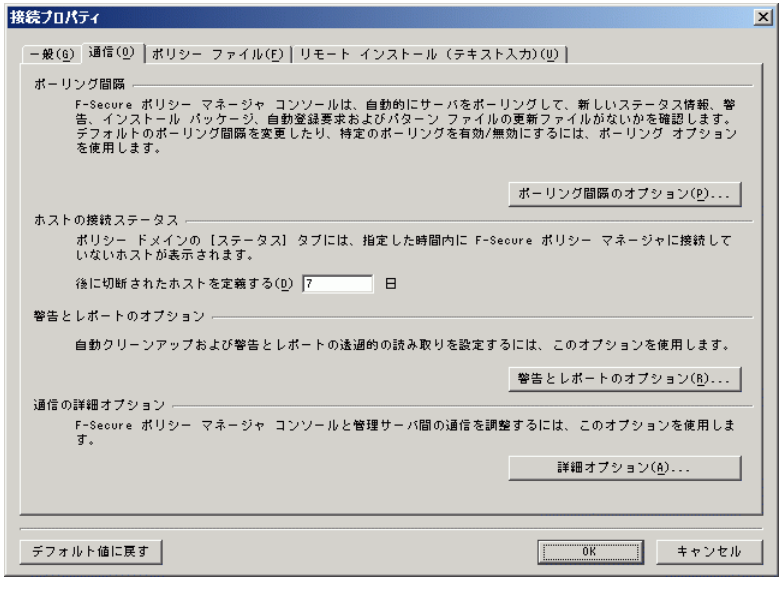


図 6-3［接続プロパティ］>［通信］ダイアログ

通信プロトコルによって、デフォルトのポーリング間隔が異なります。環境に適応するように通信設定を変更する必要があります。不要な管理情報を表示しないようにするには、無効にするポーリング項目をオフに

して、不要なポーリングをオフにする必要があります。[すべてのポーリングを無効にする] を選択すると、すべてのポーリング項目が無効になります。自動ポーリングが無効になっているかどうかにかかわらず、手動更新の操作を実行して選択したビューを更新できます。

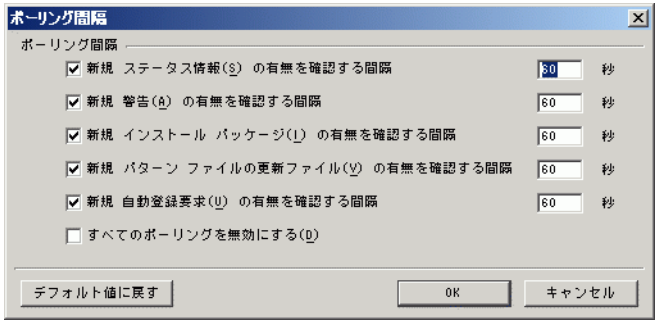


図 6-4 [ポーリング間隔] ダイアログ

接続に関する他の設定の詳細については、『一般設定』(P148) を参照してください。通常、これらの設定は、F-Secure ポリシー マネージャ コンソールの起動後に、[一般設定] ビューで編集できます。

6.2.2 ユーザ インタフェース

F-Secure ポリシー マネージャ コンソールを起動すると、ユーザ インタフェースが開きます。ユーザ インタフェースには [ポリシー ドメイン]、[プロパティ]、[製品ビュー]、[メッセージ] (メッセージがない場合は非表示) の 4 つのウィンドウが表示されます。

6.2.3 ［ポリシー ドメイン］ウィンドウ

［ポリシー ドメイン］ウィンドウでは、以下の操作を実行できます。

- 新規ポリシー ドメインの追加（ツールバーの アイコンをクリックします）。新規ポリシー ドメインは、親ドメインが選択されている場合のみ作成できます。
- 新規ホストの追加（ をクリックします）。
- ホストの検索。
- ドメインまたはホストのプロパティの表示。ホストおよびドメインには分かりやすい名前を付ける必要があります。
- 自動登録ホストのインポート。
- Windows ドメインからのホストの自動検出。
- ホストまたはドメインの削除。
- カット & ペーストを使用した、ホストまたはドメインの移動。
- ポリシー ファイルのエキスポート。

ドメインまたはホストを選択すると、［編集］メニューから上記の作業を行うコマンドを使用できます。

コマンドで参照されているドメインは、Windows NT または DNS のドメインではありません。ポリシー ドメインとは、類似のセキュリティ ポリシーが設定されているホストまたはサブドメインのグループです。

6.2.4 ［プロパティ］ウィンドウ

ポリシーの定義では、設定のデフォルト値、指定可能な値、および設定ファイルへのアクセス制約を指定します。ドメインまたはホストのプロパティは、［プロパティ］ウィンドウで定義されます。

［プロパティ］ウィンドウは、サブツリー（「ブランチ」）、テーブル、行、およびポリシー変数で構成されています。サブツリーは構造の展開のみに使用されます。テーブルには、多数の行が含まれています。

［プロパティ］ウィンドウには次のタブがあります。

- **ポリシー**
  ［製品ビュー］ウィンドウを使用して、ドメインまたはホストの設定、制約、および操作を定義できます。これらの変更は、ポリシーが配布され、エージェントがそのポリシー ファイルを取得した時点で有効になります。
- **ステータス**
  このタブに表示される各製品の下には、［設定］と［統計］の 2 つのステータス カテゴリが表示されます。［設定］には、ホストで明示的に変更されたローカルの設定が表示されます。デフォルト値や、ベース ポリシー ファイルで設定された値は表示されません。［統計］サブツリーには、各製品のホストの統計情報が表示されます。ポリシー ドメインを選択した場合、［ステータス］ビューには、ドメイン内のホスト数と、F-Secure ポリシー マネージャに接続していないホストが表示されます。
- **警告**
  選択したドメインのホストから生成された警告のリスト、［製品ビュー］ウィンドウで選択した警告、およびその警告に関連するレポートが表示されます。
- **レポート**
  選択したホストのすべてのレポートが表示されます。
- **インストール**
  インストール オプションが表示されます。

6.2.5 ［製品ビュー］ウィンドウ

［製品ビュー］ウィンドウの機能は、［プロパティ］ウィンドウで選択したタブによって異なります。

- **ポリシー**
  ［製品ビュー］ウィンドウでは、ポリシー変数の値を設定することができます。すべての変更内容は、選択したポリシー ドメインおよびホストに反映されます。各タイプのポリシー変数用にあらかじめ定義されたエディタが用意されています。［ポリシー］タブで変数のタイプを選択すると、エディタが表示されます。一部のサブツリー、テーブル、およびリーフ ノードには、特別なカスタム エディタがあります。これらのエディタに

より、インストールされている製品ごとに F-Secure ポリシー マネージャ コンソールをカスタマイズできます。制約エディタというエディタもあります。これは、[製品ビュー] ウィンドウの一部として、または個別のダイアログ ボックスとして表示されます。

- **ステータス**
  [製品ビュー] ウィンドウでは、(1) ホストによって報告されたローカルの変更を表す「設定」と、(2) 統計が表示されます。
- **警告**
  [警告] タブで警告を選択すると、警告の詳細が [製品ビュー] ウィンドウに表示されます。
- **レポート**
  [レポート] タブでレポートを選択すると、レポートの詳細が [製品ビュー] ウィンドウに表示されます。
- **インストール**
  [製品ビュー] ウィンドウでは、インストール情報を表示および編集できます。

F-Secure ポリシー マネージャ コンソールの従来の MIB ツリーでは、すべての設定 / 操作（ポリシー）とローカル設定 / 統計（ステータス）は、製品コンポーネントに固有の MIB ツリーに表示されます。また、オプションでシンプルな GUI ビューを表示することもできます。大部分の F-Secure 製品にはこれらの新しいスタイルのインタフェースがすでに定義されています。これにより、ユーザは MIB ツリーで最も重要な項目を簡単に見つけることができます。MIB ツリー形式のビューを使用してポリシーを定義したり、ステータスを表示したりすることもできますが、ほとんど場合はこの新しい製品ビューで十分です。製品ビューは MIB ツリーにもあるデータにリンクしているだけなので、MIB ツリーと製品ビューを同時に使用することもできます。

以降のページに、F-Secure 管理エージェントの製品ビューの例を示します（一般的な操作や機能はすべての製品ビューで共通です）。

ヘルプの使用

製品ビューのほとんどのフィールドには MIB ツリーのノードと同じヘルプが用意されています。また、各タブにも専用のヘルプが用意されています。ヘルプを表示するには、マウスでクリックするか（すべてのタブと、ポリシーおよびステータス エディタの場合）、フィールドにカーソルを移動します（[プロパティ] ウィンドウで [ポリシー] タブが選択されている場合）。フィールド ラベルまたは値編集フィールドをクリックすると、該当するヘルプが表示されます。

ポリシー設定の編集

F-Secure 管理エージェントなどの製品を選択し、[プロパティ] ウィンドウから [ポリシー] タブを選択します。F-Secure ポリシー マネージャ コンソールによって、選択した製品の [製品ビュー] ウィンドウに製品ビューが表示されます。このウィンドウには、MIB ツリーから選ばれた使用頻度の高い設定と制約エディタが次のカテゴリで表示されます。

- [通信] - 通信設定を編集します。
- [警告] - 警告設定を編集します。
- [警告転送] - 詳細については『*警告転送の設定*』(P142) を参照してください。
- [証明書] - 信頼済み証明書を定義します。
- [証明書ディレクトリ] - 証明書を保存するディレクトリを定義します。
- [バージョン情報] - F-Secure Web Club へのリンクがあります（詳細については、『Web Club』(P242) を参照してください）。

通常の方法でポリシー設定を編集したり、制約設定（確定、非表示）を使用してエンドユーザのアクセス権を定義したりできます。

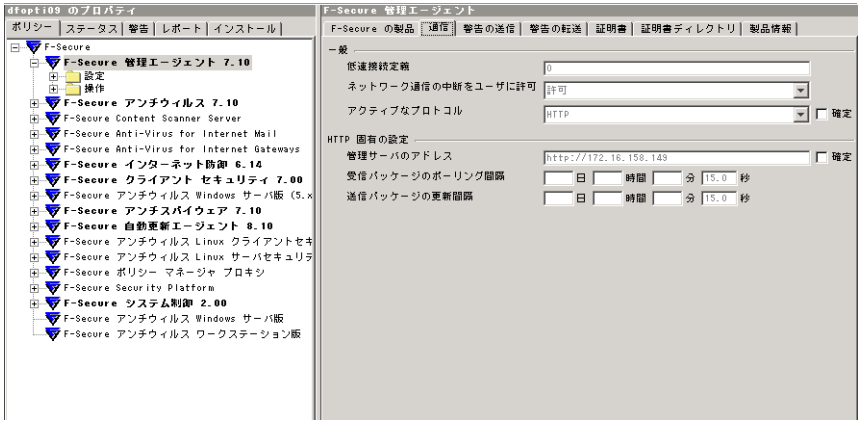


図 6-5［製品ビュー］ウィンドウ

ポリシー設定用のコンテキスト メニューの使用

製品ビューに表示されるほとんどの編集フィールドでは、コンテキスト メニューを使用できます（コンテキスト メニューはマウスを右クリックをすると表示されます）。コンテキスト メニューには［移動］、［値を消去］、［強制的に値を適用］、［ドメインの値を表示］のオプションがあります。

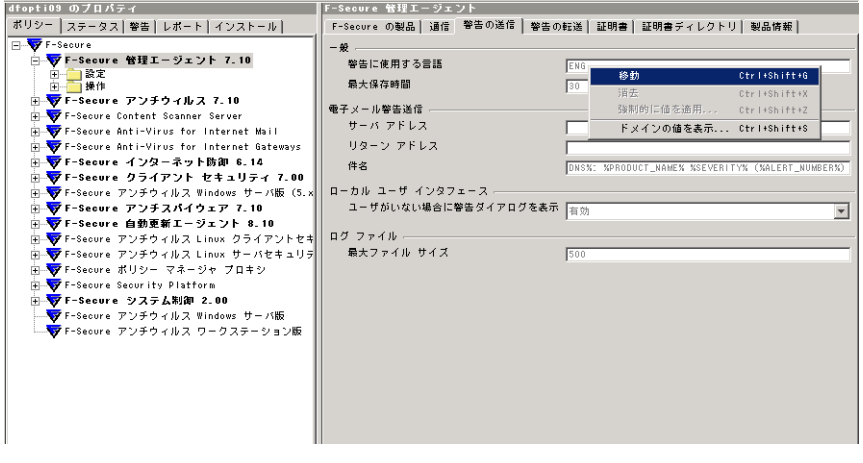


図 6-6 コンテキスト メニュー

MIB ツリー ノードへのショートカット

製品ビューの特定の項目を変更する場合、MIB ツリーのどの設定が変更されているかを確認すると便利なことがあります。[移動] メニュー項目を選択して、該当する MIB ツリー ノードを [プロパティ] ウィンドウに表示します。

MIB ツリーでは、必要性の少ないものも含めてより多くの設定パラメータが表示されます。そのため、たとえば、製品ビューに制約エディタが直接表示されないポリシー設定の制約を編集できます。

値を消去

[値を消去] メニュー項目の機能は MIB ツリーの場合と同じです。現在の値を消去すると、フィールドには継承された値（グレーのテキスト）が表示されるか、何も表示されません。[値を消去] メニュー項目を使用できるのは、現在定義されているドメインまたはホストに対して値が定義されている場合だけです。

強制的に値を適用

[強制的に値を適用] メニュー項目は、ポリシー ドメインが選択されている場合にのみ使用できます。現在のドメイン設定をすべてのサブドメインとホストにも強制的に適用できます。実際には、この操作は、現在のドメインの下にあるすべてのサブドメインとホストから対応する設定を消去して、すべてのサブドメインとホストに現在の値を継承できるようにします。このメニュー エントリは慎重に使用してください。選択されたドメイン下のサブドメインまたはホストで定義された値はすべて破棄され、復元することはできません。

ドメインの値を表示

[ドメインの値を表示] メニュー項目は、ポリシー ドメインを選択した場合に限り利用可能です。選択したポリシー ドメインの下にあるすべてのポリシー ドメインとホストのリストと、選択したフィールドの値を表示できます。

ドメイン名やホスト名をクリックすると、[ポリシー ドメイン] ウィンドウでドメインやホストを簡単に選択できます。ドメインの値の複数のダイアログを同時に開くことができます。

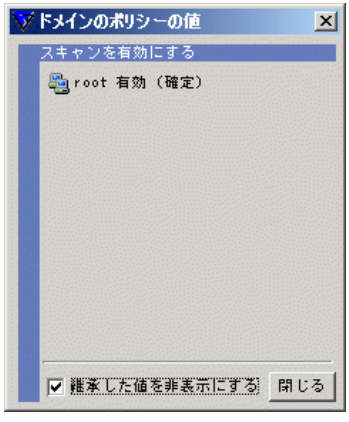


図 6-7 [ドメインの値を表示] ダイアログ

ステータスの表示

[ステータス] タブを開いて、[プロパティ] ウィンドウから製品を選択します。F-Secure ポリシー マネージャ コンソールの [製品ビュー] ウィンドウに製品ビューが表示され、重要なローカル設定と統計を参照できます。

値を編集することはできませんが、フィールドまたはフィールドラベルをクリックして MIB ヘルプを表示することはできます。

ポリシー ドメインの場合、[ステータス] タブには、ドメイン レベルのステータス概要 (ドメイン内のホスト数と、切断されたホストのリスト) が表示されます。

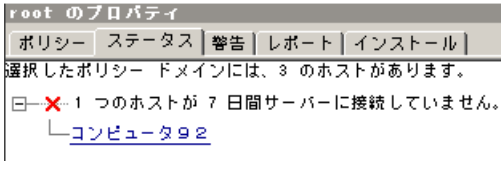


図 6-8 [ステータス] タブ

切断されたホストをクリックすると、そのホストのポリシー ドメインが選択されます。これにより、切断されたホストが切断前に警告や有用な統計を送信したかどうかを調査できます。この情報は、ホストが切断された理由を調査する場合に役立つことがあります。ホストの

F-Secure ソフトウェアがアンインストールされたなど、理由が明らかな場合は、通常の手順でホストを削除できます。切断されたホストの調査が終わったら、ツールバーの ⇦ ボタンをクリックすると、以前に選択していたドメイン レベルに簡単に戻ることができます。

切断されたホストの数が多い場合に一括して処理できるよう、[ドメインのステータス] ビューには 2 種類のショートカット操作があり、切断されたすべてのホストを選択したり、切断されたすべてのホストを削除したりすることができます。どちらの操作も、[切断されたホスト] ツリーのルート ノードのコンテキスト メニューからアクセスできます。

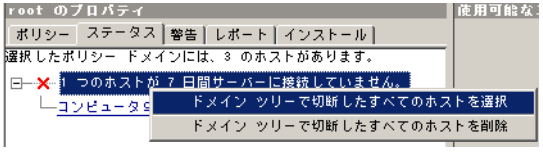


図 6-9 [ドメインのステータス] ビューで使用できるショートカットの例

警告 ： 切断されたすべてのホストを削除する操作には危険が伴います。一部の既存のホストは、その性質上、割り当てられているしきい値日数より長い間、一時的に切断されている場合があるからです。ホストを削除する前に、[一般設定] の切断しきい値を必ず確認してください。既存のホストを誤って削除した場合、そのホストに固有の警告、レポート、ステータス、およびポリシー設定はすべて失われます。ただし、ホストは F-Secure ポリシー マネージャから削除されたことを感知すると自動登録メッセージを送信します。ホストをドメイ ンツリーに再インポートすることはできますが、ポリシー マネージャでは新しく追加されたホストと見なされます。

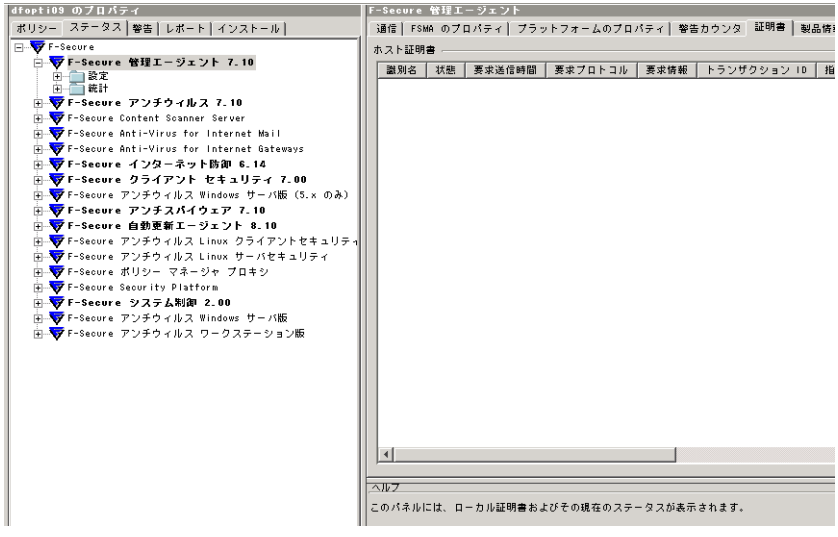


図 6-10［製品ビュー］ウィンドウに表示されるコンポーネントのステータス

6.2.6 ［メッセージ］ウィンドウ

F-Secure ポリシー マネージャ コンソールは、さまざまなイベントのメッセージのログを［メッセージ］ウィンドウに出力します。［警告］ウィンドウや［レポート］ウィンドウと異なり、［メッセージ］ウィンドウのイベントは F-Secure ポリシー マネージャ コンソールによってのみ生成されます。

メッセージには、情報、警告、およびエラーの 3 つのカテゴリがあります。各［メッセージ ビュー］タブには 3 段階の重大度すべてのメッセージが表示されます。コンテキスト メニューに表示されているカテゴリは、タブを右クリックすることで削除できます。各メッセージを右クリックすると、切り取り、コピー、および削除機能が表示されたコンテキスト メニューが表示されます。

デフォルトでは、メッセージは、F-Secure ポリシー マネージャ コンソールのローカル インストール先ディレクトリの message サブディレクトリ内にある UTF-8 ファイルに記録されます。メッセージ カテゴリ（［メッセージ］ウィンドウのタブ名）ごとに個別のログ ファイルが作成されます。［一般設定］の［場所］ページを使用して、ログ ファイ

ルのディレクトリを指定し、ログ機能のオン / オフを切り換えることができます。また、メッセージの保存機能のオン / オフも、メッセージビューの機能に影響を与えません。

6.2.7 ツールバー

ツールバーには、F-Secure ポリシー マネージャ コンソールの一般的なタスクを実行するためのボタンが表示されます。.

	ポリシー データを保存します。
	ポリシーを配布します。
	ドメイン ツリーの選択履歴で前のドメインまたはホストに移動します。
	ドメイン ツリーの選択履歴で次のドメインまたはホストに移動します。
	親ドメインに移動します。
	ホストまたはドメインを切り取ります。
	ホストまたはドメインを貼り付けます。
	現在選択されているドメインに、ドメインを追加します。
	現在選択されているドメインに、ホストを追加します。
	ホストまたはドメインの［プロパティ］ボックスを表示します。

Windows ホストの自動検出ツールが起動されます。現在選択されているポリシー ドメインに新しいホストが追加されます。

Windows ホストへのインストール情報の送信を開始します。

現在選択されているドメインに、自動登録ホストをインポートします。緑色は、ホストから自動登録要求が送信されたことを示しています。

使用可能なインストール パッケージを表示します。

パターン ファイルを更新します。

すべての警告を表示します。新しい警告がある場合、アイコンが強調表示されます。F-Secure ポリシー マネージャ コンソールの起動時には、アイコンが必ず強調表示されます。

6.2.8 メニュー コマンド

メニュー	コマンド	アクション
ファイル	新規	MIB（マネージメント インフォメーション ベース）のデフォルト値を使用して新しいポリシー データを作成します。通常、既存のポリシー データを変更して、[名前を付けて保存] コマンドで保存して使用するため、このコマンドはほとんど必要ありません。
	開く	保存されているポリシー データを開きます。
	保存	現在のポリシー データを保存します。
	名前を付けて保存	名前を指定してポリシー データを保存します。
	配布	ポリシー ファイルを配布します。
	ポリシー ファイルのエキスポート	ポリシー ファイルをエキスポートします。
	終了	F-Secure ポリシー マネージャ コンソールを終了します。
編集	切り取り	選択したアイテムを切り取ります。
	貼り付け	選択した場所にアイテムを貼り付けます。
	削除	選択したアイテムを削除します。
	新規ポリシー ドメイン	新しいドメインを追加します。
	新規ホスト	新しいホストを追加します。
	自動登録ホストのインポート	自動登録要求を送信したホストをインポートします。
	Windows ホストの自動検出	Windows ドメイン構造からホストをインポートします。
	Windows ホストへのインストール情報の送信	ソフトウェアをリモートでインストールし、IP アドレスまたは WINS 名で指定したホストをインポートします。
	検索	ホストのプロパティで文字列を検索します。選択したドメイン内のすべてのホストが検索されます。
	プロパティ . . .	選択したホストまたはポリシー ドメインの [プロパティ] ページを表示します。
表示	ツール バー	ツールバーを表示します。

	ステータス バー	ステータス バーを表示します。
	ツールヒント (T)	マウス ポインタをボタン上に置くと、そのボタンの説明が画面に表示されます。
	組み込み制約エディタ (E)	組み込み制約エディタと制約ダイアログ ボックスを切り換えます。
	メッセージ	画面の下部に表示される［メッセージ］ウィンドウの表示 / 非表示を切り替えます。
	前のドメイン / ホスト	ドメイン ツリーの選択履歴で前のドメインまたはホストに移動します。
	次のドメイン / ホスト	ドメイン ツリーの選択履歴で次のドメインまたはホストに移動します。
	親ドメイン (P)	親ドメインに移動します。
	すべての警告 (A)	［プロパティ］ウィンドウの［警告］ページを開き、すべての警告を表示します。
	詳細モード (D)	詳細モードのユーザ インタフェース（本マニュアルで説明しているユーザ インタフェース）に変更します。
	アンチウィルス モード (I)	アンチウィルス モードのユーザ インタフェースに変更します。このユーザ インタフェースは、F-Secure クライアント セキュリティの集中管理に最適化されています。
	〈項目名〉の再表示	ステータス、警告、またはレポート ビューをマニュアルで再表示します。プロパティ ウィンドウで選択されているタブに従って、異なるメニュー項目が表示されます。
	すべて再表示 (L)	ポリシー、ステータス、警告、レポート、インストール パッケージ、および自動登録要求などのインタフェースに影響を与えるすべてのデータをマニュアルで更新します。
ツール	インストール パッケージ	インストール パッケージの情報をダイアログ ボックスに表示します。
	パスワードの変更	ログイン パスワード (F-Secure ポリシー マネージャ コンソールの秘密鍵を保護するパスワード) を変更します。
	レポート	レポート方法と、レポートに含めるドメイン / ホストおよび製品を選択できます。
	パターン ファイルの更新	サーバ上のパターン ファイルを ZIP ファイルからインポートします。

	一般設定	F-Secure ポリシー マネージャ コンソールのローカル プロパティを設定します。これらの設定は、F-Secure ポリシー マネージャ コンソールのローカル インストールのみに影響します。
ヘルプ	目次	ヘルプの目次を表示します。
	Web Club(W)	Web ブラウザを開き、F-Secure ポリシー マネージャ Web Club に接続します。
	お問い合わせ先	F-Secure Corporation の連絡先を表示します。
	F-Secure ポリシー マネージャ コンソールについて	バージョン情報を表示します。

6.3 F-Secure クライアント セキュリティの管理

F-Secure ポリシー マネージャ 5.50 以降では、F-Secure クライアント セキュリティと F-Secure アンチウィルス ワークステーション版の管理用に、独立した新しいグラフィカル ユーザ インタフェースが採用されています。この新しいユーザ インタフェースは、ウィルス保護、自動更新、電子メール スキャン、およびインターネット防御（アプリケーション制御、ファイアウォール、侵入検知システムを含む）という F-Secure クライアント セキュリティの各機能を集中管理するために最適化されています。

このユーザ インタフェースを開くには、[表示] メニューの [アンチウィルス モード] を選択します。

詳細については、『F-Secure クライアント セキュリティ管理者用ガイド』を参照してください。

6.4 ドメインとホストの管理

ホストを F-Secure ポリシー マネージャへインポートする前に、ポリシー ドメインの構造を設計する必要があります。以下に、ドメイン / サブドメイン レベルのポリシー ドメイン構造の例を示します。F-Secure 管理エージェントをホストにインストールすると、個々のホストをこの構造にインポートできます。

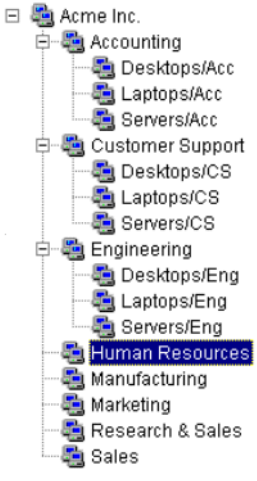


図 6-11 ポリシー ドメイン構造の例

すべてのドメインとホストには、構造内で一意の名前を付ける必要があります。

6.4.1 ポリシー ドメインの追加

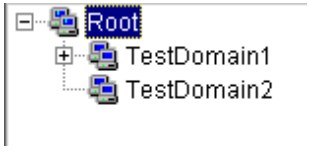


図 6-12 サブドメインがあるポリシー ドメインの例

［編集］メニューから［新規ポリシー ドメイン］を選択します（親ドメインを選択する必要があります）。あるいは、ツールバーにある をクリックします（または Ctrl+Insert を押します）。新しいポリシー ドメインは、選択した親ドメインのサブドメインになります。

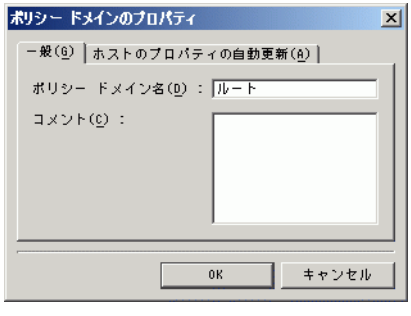


図 6-13［ポリシー ドメインのプロパティ］ダイアログ

ポリシー ドメインの名前を入力するよう要求されます。ドメインのアイコンが［ポリシー ドメイン］ウィンドウに作成されます。

6.4.2 ホストの追加

ポリシー ドメインへのホストの追加には、使用しているオペレーティング システムに応じて、主に次の 3 つの方法があります。

- Windows ドメインから直接ホストをインポートする方法。
- ホストを自動登録でインポートする方法（そのホストに F-Secure 管理エージェントがインストールされている必要があります）。別の条件を使用して、自動登録ホストを別のサブドメインにインポートすることもできます。
- ［新規ホスト］コマンドを使用して、手動でホストを作成する方法。

Windows ドメイン

Windows ドメインの場合、ポリシー ドメインにホストを追加する最も便利な方法は、F-Secure ポリシー マネージャ コンソールの［編集］メニューから［Windows ホストの自動検出］を選択して、F-Secure インテリジェント インストールでインポートする方法です。この方法では、インポートしたホストに F-Secure 管理エージェントがインストールされます。Windows ドメインからホストをインポートするには、インポート先のドメインを選択し、［編集］メニューから［Windows ホストの自動検出］を選択します。自動検出処理が完了すると、新しいホストが自動的にポリシー ドメイン ツリーに追加されます。詳細については、『ソフトウェアの配布』(P115) を参照してください。

自動登録ホスト

ホストを F-Secure ポリシー マネージャ コンソールにインポートするもう 1 つの方法は、自動登録機能を使用する方法です。この方法は、F-Secure 管理エージェントがホストにインストールされていて、ホストが自動登録要求を送信した後にのみ実行できます。F-Secure 管理エージェントは、CD-ROM やログイン スクリプトなどを使用してインストールする必要があります。自動登録ホストをインポートするには、 をクリックするか、［編集］メニューから［自動登録ホストのインポート］を選択します。操作が完了すると、ホストがドメイン ツリーに追加されます。異なる条件（ホストの IP アドレスや DNS アドレスなど）

を指定すると、自動登録ホストを別のドメインにインポートできます。詳細については、『自動登録のインポート ルール』(P108) を参照してください。

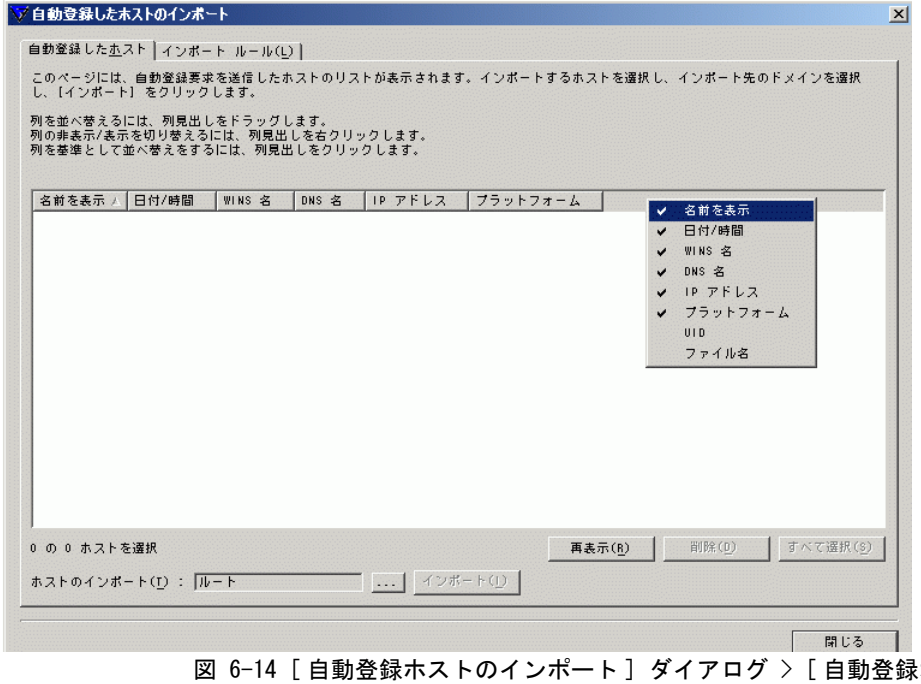


図 6-14 [自動登録ホストのインポート] ダイアログ > [自動登録ホスト] タブ

[自動登録] ビューには、ホストが自動登録メッセージで送信するデータが表形式で表示されます。テーブルには、インストール時にリモート インストール パッケージに含まれていた有効なカスタム自動登録プロパティが含まれます (『カスタマイズしたリモート インストール JAR パッケージの使用』(P129) の手順 6 を参照)。対応するテーブル ヘッダーをクリックすると、列の値に基づいて自動登録メッセージを並べ替えることができます。列を並べ替えるには、適切な位置に列をドラッグ アンド ドロップします。また、列の幅は自由に調整することができます。テーブルのコンテキスト メニュー (テーブルのヘッダー バーを右クリック) は、自動登録プロパティをテーブルに表示するかどうかを指定する場合に使用されます。

自動登録のインポート ルール

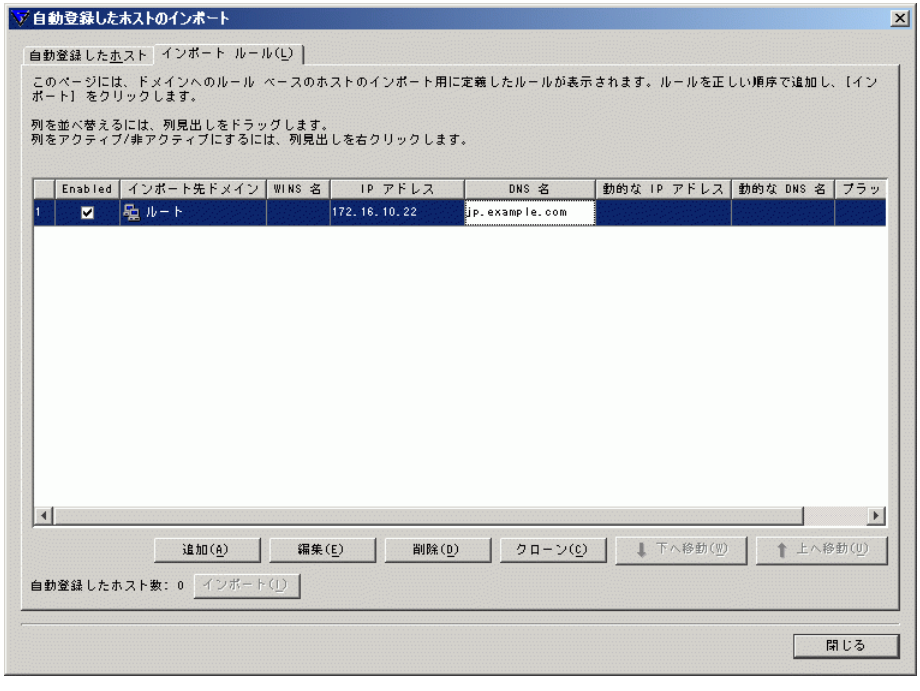


図 6-15 [自動登録ホストのインポート] ダイアログ > [インポート ルール] タブ

[自動登録ホストのインポート] ウィンドウの [インポート ルール] タブで、自動登録ホストのインポート ルールを定義できます。ルールのインポート条件として、以下を使用できます。

- [WINS 名]、[DNS 名]、[動的な DNS 名]、[カスタム プロパティ]
  - ワイルドカードとして *（アスタリスク）がサポートされています。* は、任意の数の文字を表すことができます。例 :host_test* または *.example.com。
  - 大文字と小文字は区別されません。そのため、大文字と小文字は同じ文字として扱われます。
- [IP アドレス]、[動的な IP アドレス]

- これらは、正確な IP アドレスの一致（例： 192.1.2.3）、および IP サブドメインの一致（例： 10.15.0.0/16）をサポートします。

［インポート ルール］ウィンドウで列の見出しを右クリックしたときに開く右クリック メニューを使用すると、テーブルで列を表示および非表示することができます。現在表示されている列の値だけが、ポリシー ドメインにホストをインポートする時の一致条件として使用されます。現在非表示となっている列の値は無視されます。

また、新しいカスタム プロパティを追加して、ホストのインポート時の条件として使用することもできます。カスタム プロパティの使用方法の例として、ユニット固有のポリシー ドメイン下でグループ化する必要がある異なる組織ユニットに対して、個別のインストール パッケージを作成する方法があります。この場合、ユニット名をカスタム プロパティとして使用し、インポート条件としてユニット名を使用するインポート ルールを作成する必要があります。非表示になっているカスタム プロパティ名はコンソールが開かれている間だけ記憶されています。

新しいカスタム プロパティを追加するには、以下の手順を実行します。

1. 列の見出しを右クリックして、［新しいカスタム プロパティの追加］を選択します。［新しいカスタム プロパティ］ダイアログが開きます。
2. カスタム プロパティの名前を入力します（例えば、ユニット名）。［OK］をクリックします。
3. これで、新しいカスタム プロパティがテーブルに表示され、インポート条件として使用する新しい自動登録のインポート ルールを作成できます。

新しい自動登録のインポート ルールを作成するには、以下の手順を実行します。

1. ［インポート ルール］タブで［**追加**］をクリックします。既存のドメインおよびサブドメインを表示する［ルールのインポート先ポリシー ドメインの選択］ダイアログが開きます。
2. ルールを作成するドメインを選択して、［OK］をクリックします。
3. これで、インポート条件を定義できます。作成された新しい列を選択して、値を追加するセルをクリックし、［**編集**］をクリックします。セルに値を入力します。

自動登録ホストがインポートされると、ルールが上から順番に検証され、最初に一致するルールが適用されます。[**下へ移動**] または [**上へ移動**] をクリックすると、ルールの順番を変更できます。

ドメインのルールを複数作成する場合は、[**クローン**] オプションを使用します。まず、ドメインのルールを 1 つ作成します。次に、列を選択して [**クローン**] をクリックします。これで、新しく複製された列で条件を編集できます。

インポート処理を開始する場合は、[自動登録ホスト] タブで [**インポート**] をクリックします。定義したインポート ルールが、インポートの開始前に検証されます。ホストがインポートされると、正常にインポートされたホストの数および失敗したインポート操作の数を示す [概要] ダイアログが表示されます。

条件セットを空白にすると、常に一致するとみなされます。

ホストを手動で作成する

ホストを手動で作成するには、ポリシー ドメインを選択して、[編集] メニューから [新規ホスト] を選択するか、[**ホストの追加**] ボタンをクリックします（または Insert キーを押します）。この操作は、次の場合に役立ちます。

使用方法の習得およびテスト
F-Secure ポリシー マネージャ コンソールの他にソフトウェアをインストールすることなく、F-Secure ポリシー マネージャ コンソールの機能のサブセットを使用することができます。たとえば、テスト ドメインとホストを作成し、F-Secure VPN+ を複数のホストにインストールすることなく、F-Secure VPN+ 接続を定義できます。

ポリシーの事前定義
ソフトウェアをホストにインストールする前に、ホストのポリシーを定義および生成できます。

特別な場合
サーバに直接アクセスしないホストのポリシーを生成できます（つまり、ホストをインポートできない場合）。たとえば、通信ディレクトリにアクセスしない VPN+ ゲートウェイのベース ポリシー ファイルを生成できます。ベース ポリシー ファイルは、手動でまたは他の外部転送メカニズムを使用して転送する必要があります。この操作を行うには、[編集] メニューから [ポリシー ファイルのエキスポート] を選択します。

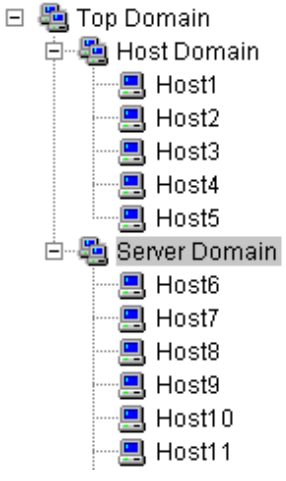


図 6-16 独自のサブドメインを持つホストおよびサーバで構成されるドメインの例

F-Secure 管理エージェントがインストールされていないホストはポリシーを取得できないため、F-Secure ポリシー マネージャ コンソールを使用して管理することはできません。また、ステータス情報も表示されません。
ドメイン構造の変更を現在のポリシー データに保存しないで F-Secure ポリシー マネージャ コンソールを終了しても、その変更内容は実装されます。

6.4.3 ホストのプロパティ

ネットワークのホスト名には、IP アドレス、ドメイン名、または WINS 名を使用できます。ホストのプロパティを表示するには、目的のホストを右クリックして、表示されるメニューから［プロパティ］を選択します（または Alt+Enter キーを押します）。ホストのプロパティを変更するには、［ホストのプロパティ］ダイアログ ボックスで［ID］タブの［自動更新のプロパティ］チェックボックスをオフにします。［編集］メニューから［プロパティ］を選択するか、ツールバーで をクリックすると、［ホストのプロパティ］ダイアログ ボックスが表示されます。

ホストのネットワーク名は、ホストがポリシーにアクセスするためにネットワーク内部で使用している名前です。

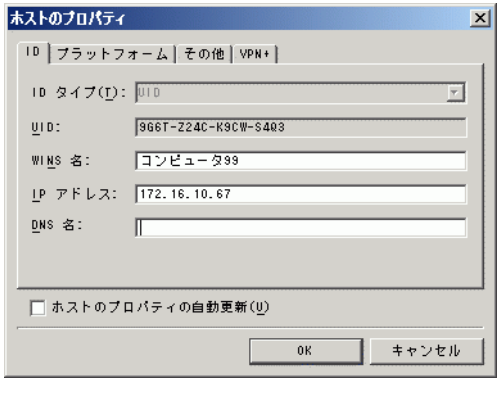


図 6-17［ホストのプロパティ］ダイアログ

［プラットフォーム］タブでホストのオペレーティング システムをプロパティに追加することができます。「プラットフォーム名」はオペレーティング システムの名前です。オペレーティング システムのバージョン番号は、以下のとおりです。

Windows 95	4.0
Windows 98	4.1/4.10
Windows Me	4.9

Windows NT 4.0	4.0
Windows 2000	5.0
Windows XP	5.1/5.10

ホストのエイリアスは、[その他] タブで定義できます。エイリアスが定義されている場合、ドメイン ツリーには、元のホストの代わりにエイリアスが表示されます。

[VPN+] タブは、F-Secure VPN+ ソフトウェアがインストールされている場合のみ使用します。[VPN+] タブには、ホストの VPN+ ID に関する情報（IPSec 接続で使用）が含まれています。

ホストが固定 IP アドレスを使用していない場合、つまりダイヤルアップ ホストが DHCP を使用して IP アドレスを取得している場合は、電子メール アドレスを VPN+ ID として使用する必要があります。サーバとゲートウェイについては、常に固定 IP アドレスを使用し、VPN+ ID として IP アドレスを使用します。

VPN+ ID の自動初期化

VPN+ ID は、他のホストのプロパティと同様、プロパティの自動更新をサポートしています。ただし、空になっているプロパティを自動的に初期化する機能もあります。

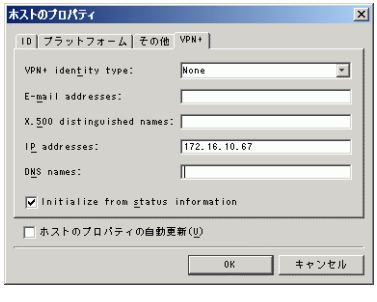


図 6-18 [ホストのプロパティ] > [VPN+] ダイアログ

［ステータス情報から初期化］チェックボックスをオンにしている場合、VPN+ のプロパティは、ホストから送信されるステータス情報を使用して初期化されます。以下の初期化が実行されます。

- ［VPN+ ID のタイプ］フィールドの値が［なし］になっている場合、すべての ID タイプが初期化されます。
- ［電子メール アドレス］フィールドが空の場合、このフィールドは初期化されます。
- ［X.500 識別名］フィールドが空の場合、このフィールドは初期化されます。

自動初期化は、元のホストのプロパティに VPN+ ID の情報が含まれていない場合に便利です。自動初期化は、以下のような場合に実行されます。

- ホストが Windows ドメインからインポートされる場合（F-Secure 管理エージェントがリモートでインストールされている場合）。VPN+ がインストールされていないため、VPN+ ID に関する情報は取得できません。VPN+ はポリシーベース インストールを使用してインストールされます。VPN+ ID およびその情報が統計に書き込まれたことが、ホストで確認されます。ホストの統計情報に VPN+ ID が含まれていることが、F-Secure ポリシー マネージャ コンソールで確認されます。［ステータス情報から初期化］チェックボックスがオンになっている場合、ホストのプロパティは前述したように初期化され、F-Secure ポリシー マネージャ コンソールの［メッセージ］ウィンドウに通知が表示されます。

自動更新と自動初期化の主な違いは、自動初期化は一度しか実行されないということです。自動更新では、値が元々手動で入力された場合でも、必ずプロパティは更新されます。自動初期化はさらに制限されています。フィールドに値がある場合、その値は変更されません。初期値がホストの統計から取得されたものであるか、手動で定義されたものであるかは、関係ありません。

6.5 ソフトウェアの配布

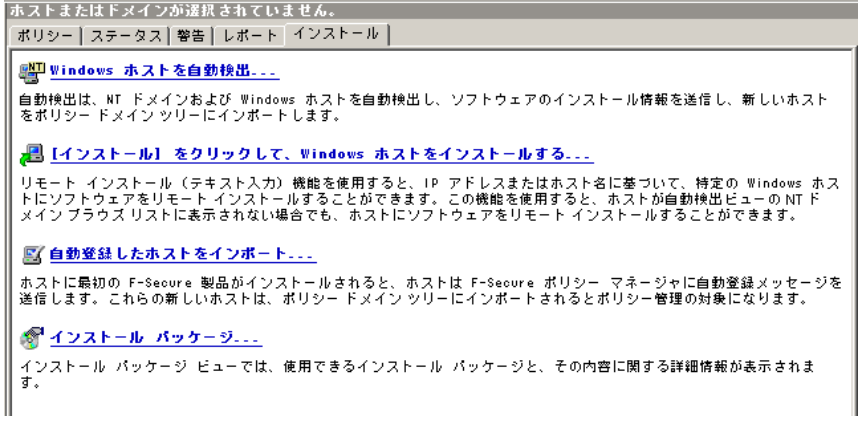
F-Secure ポリシー マネージャでは、次の方法で管理対象アプリケーションのインストールと更新を行うことができます。

- **インストール情報の送信**
  F-Secure ポリシー マネージャを使用して、まだ集中管理されていない新しいホストにソフトウェアをインストールできます。[Windows ホストの自動検出] 機能を使用してホストを参照するか、または [Windows ホストへのインストール情報の送信] 機能を使用して、対象となるホストを WINS 名または IP アドレスで直接指定できます。インストール情報送信機能は、最初のインストール時以外にも、ポリシー ベース インストールを使用できない場合にインストール済みのソフトウェアを更新または修復するために使用できます。
- **ポリシー ベース インストール**
  F-Secure ポリシー マネージャは、ポリシー ベースのトリガを使用したインストール処理と更新処理を実行できます。この機能を使用するには、ホストがすでに集中管理されている（つまり、F-Secure ポリシー マネージャ コンソールのポリシー ドメインに含まれている）必要があります。
- **CD-ROM からローカルでインストールおよび更新**
  CD-ROM から直接セットアップ プログラムを実行することで、ホストに単独でインストールを実行できます。インストールの完了後、F-Secure 管理エージェントは F-Secure ポリシー マネージャに登録メッセージを送信します。管理者は、F-Secure ポリシー マネージャ コンソールの [編集] メニューから [自動登録ホストのインポート] コマンドを選択して新規ホストを表示し、受け付けることができます。
- **設定済みパッケージを使用してローカルでインストールおよび更新**
  標準の CD-ROM のセットアップを使用する代わりに、F-Secure ポリシー マネージャを使用して、インストールで使用する設定情報が含まれているカスタマイズされたインストール パッケージ（JAR）を準備することができます。設定済みのパッケージに

は、通常ユーザが要求するすべての設定が含まれているため、これを使用してエンドユーザのコンピュータをサイレント モードで設定できます。

- **F-Secure パターン ファイル更新**
  F-Secure ポリシー マネージャで、F-Secure の自動更新サイトから最新のパターン ファイルを自動的にダウンロードして、更新することができます。管理対象ホストは、ホストのポリシーに従って F-Secure ポリシー マネージャから更新ファイルを取得します。この処理は、自動的に実行するか、またはリモート操作で開始できます。詳細については、『F-Secure 自動更新エージェントによる自動更新』(P162) を参照してください。

インストールに関連するすべての機能のショートカットは、[インストール] タブの [プロパティ] ウィンドウに集められています。



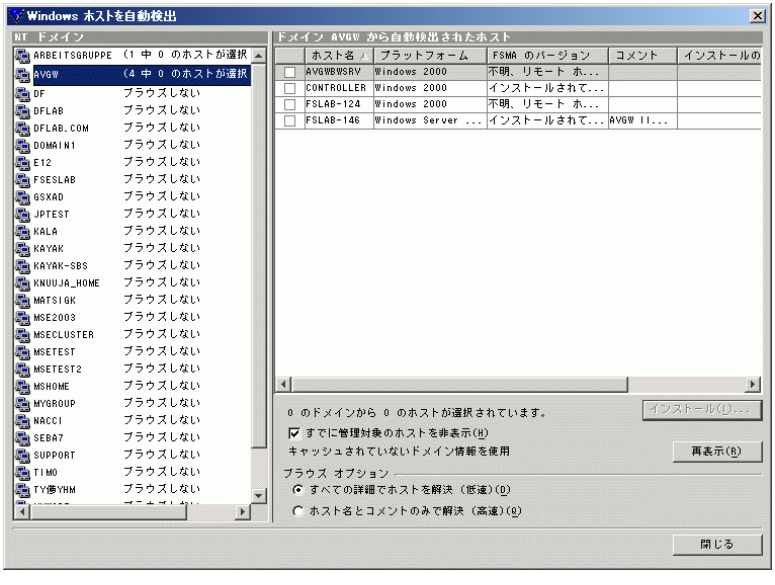
6.5.1 F-Secure によるインストール情報の送信

[Windows ホストの自動検出] と [Windows ホストへのインストール情報の送信] 機能の違いは、インストール先ホストの選択方法のみです。自動検出機能では、Windows ドメインを参照して、ホストのリストから対象ホストを選択します。[Windows ホストへのインストール情報の送信] 機能では、IP アドレスまたはホスト名を直接指定して対象ホストを設定します。インストール先ホストを選択すると、インストール情報の送信操作はどちらも同じ方法で続行されます。

Windows ホストの自動検出

インストールするには、以下の手順を実行します。

1. F-Secure 管理エージェントをインストールするホストのポリシードメインを選択します。
2. ［編集］メニューを開いて、[Windows ホストの自動検出］を選択します（または ボタンをクリックします）。



3. NT ドメインのリストからドメインの 1 つを選択して、［**再表示**］をクリックします。

   ホストのリストは、［**再表示**］をクリックした場合に限り更新されます。パフォーマンス上の理由により、［再表示］をクリックしなかった場合はキャッシュされている情報が表示されます。［**再表示**］をクリックする前に、以下の自動検出のオプションを変更できます。

   すでに管理対象のホストを非表示

   - F-Secure アプリケーションが**インストールされていない**ホストだけを表示するには、［すでに管理対象ホストを非表示］チェックボックスをオンにします。

すべての詳細でホストを解決（低速）

- このオプションを選択すると、オペレーティング システムおよび F-Secure 管理エージェントのバージョンなど、ホストに関する詳細がすべて表示されます。

ホスト名とコメントのみで解決（高速）

- このオプションは、詳細ビューにすべてのホストが表示されていない場合、またはリストの取得に時間がかかり過ぎる場合に使用します。マスター ブラウザがネットワークに最近インストールした新しいホストを検出するまでに多少時間がかかることがあります。

4. インストールするホストを選択します。選択されたホストにチェックマークを付けるには、Space キーを押します。

   Shift キーを押した状態で以下のいずれかの操作を実行すると、複数のホストを簡単に選択できます。

   - 複数のホストの列をクリック
   - マウスを複数のホストの列上でドラッグ
   - 上下矢印キーを使用

   また、マウスを右クリックすることもできます。以下を選択するには、ホストのリストのコンテキスト メニューを使用します。

   - [オン] - 選択したホストにチェック マークを付けます（Space キーを押した場合と同じです）。
   - [オフ] - 選択したホストのチェック マークを解除します（Space キーを押した場合と同じです）。
   - [すべてオン] - 選択した Windows ドメインのすべてのホストにチェック マークを付けます。
   - [すべてオフ] - 選択した Windows ドメインのすべてのホストのチェック マークを解除します。

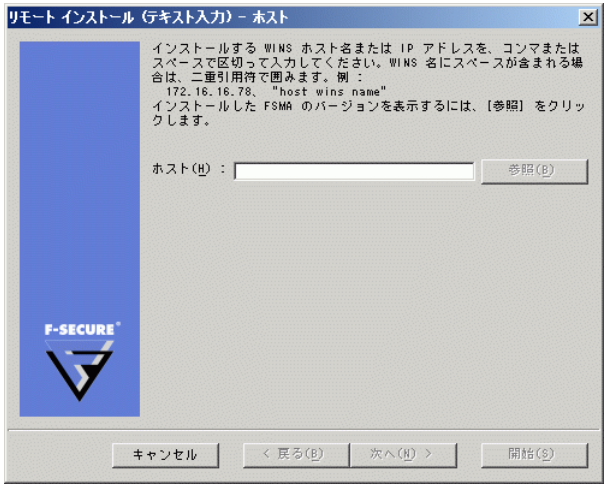
   [**インストール**] をクリックして次に進みます。

5. インストール先のホストを選択したら、『インストール先ホスト選択後のインストール情報の送信』(P119) に進み、ホストにアプリケーションのインストール情報を送信する手順を実行します。

Windows ホストへのインストール情報の送信

インストールするには、以下の手順を実行します。

1. F-Secure 管理エージェントをインストールするホストのポリシー ドメインを選択します。
2. [編集] メニューを開いて、[Windows ホストへのインストール情報の送信] を選択します（または ボタンをクリックします）。
3. インストール情報を送信するホストのインストール先ホスト名を入力して、[**次へ**] をクリックして進みます。
   [**参照**] をクリックすると、ホスト上の F-Secure 管理エージェントのバージョンを確認できます。

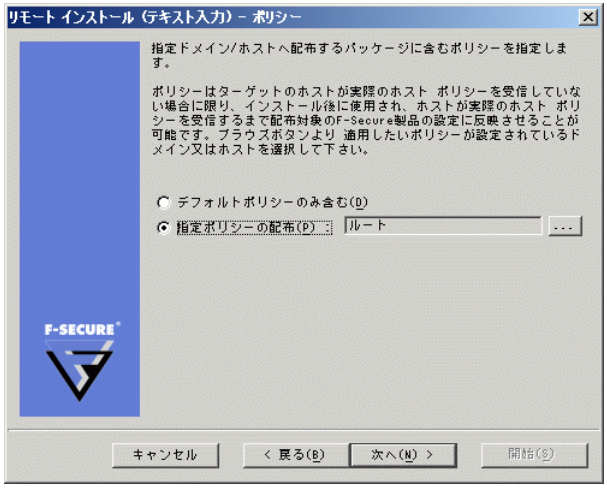


4. インストール先のホストを選択したら、『インストール先ホスト選択後のインストール情報の送信』(P119) に進み、ホストにアプリケーションのインストール情報を送信する手順を実行します。

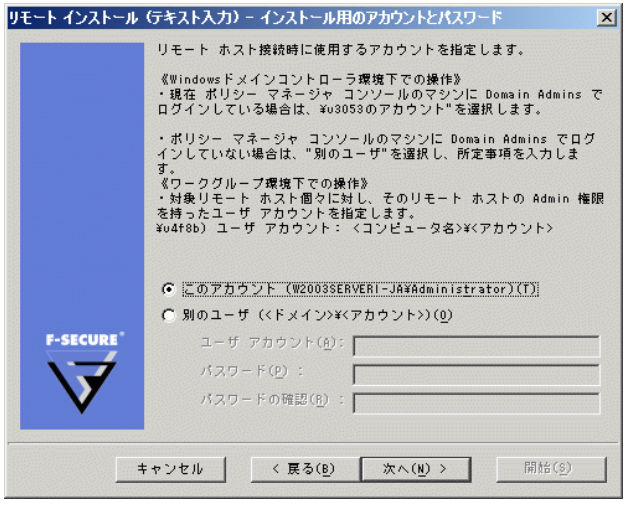
インストール先ホスト選択後のインストール情報の送信

インストール先ホストを選択した後で、インストール パッケージのインストール情報を送信するには、以下の手順を実行します。

1. インストール パッケージを選択し、[次へ] をクリックして次に進みます。
2. インストールする製品を選択します。同じバージョン番号のアプリケーションがすでに存在する場合は、強制的に再インストールを選択できます。[次へ] をクリックして次へ進みます。
3. デフォルト ポリシーの使用を選択するか、匿名ポリシーとして使用する必要があるホストまたはドメイン ポリシーを指定します。[次へ] をクリックして次へ進みます。



4. インストール情報の送信で使用するユーザ アカウントとパスワードを選択します。



インストール情報の送信には、インストール先マシンの管理者権限が必要になります。ログインしたアカウントがいずれかのリモート ホストの管理者権限を持っていない場合、そのホストに対して「アクセスは拒否されました」というエラー メッセージが表示されます。この場合、他のホストでのインストールは続行されます。

[**このアカウント**]（現在のアカウント）または [**別のアカウント**] を選択します。

このアカウント
現在ログオンしているアカウントのセキュリティ権限を使用します。このオプションは、以下のいずれかの場合に使用します。

a. ドメイン管理者としてすでにログインしている。

b. インストール先ホストに、ローカル管理者のパスワードを使用してローカル管理者としてログインしている。

別のアカウント
アカウントとパスワードを入力します。

管理者は、適切なドメイン管理者のアカウントとパスワードを入力して、選択したホストで簡単にリモート インストールを完了できます。

ドメイン アカウントで信頼済みドメインおよび信頼されていないドメインへのインストールを完了する場合は、必ず DOMAIN¥ACCOUNT の形式でアカウントを入力してください。

ローカル管理者アカウントを使用する場合は、ACCOUNT の形式を使用してください。（アカウントの一部としてホスト名を入力しないでください。ホスト名を入力すると、そのアカウントは指定のホストにしか認識されません）。

インストール時に管理者のマシンが別のユーザ アカウントでインストール先マシンにネットワーク接続を確立すると、NT 証明書の競合エラー メッセージ 1219 が表示されます。この場合、現在行われている接続を閉じてから、インテリジェント インストールを実行します。

5. インストールの概要を確認します。リモート インストール ウィザードを起動するには、[**開始**] をクリックします。

   リモート インストール ウィザードでは、一連のダイアログ ボックスを通してインストールの実行に必要ないくつかの質問に答えていきます。最後のダイアログ ボックスで [**完了**] をクリックして、次の手順に進みます。

6. F-Secure ポリシー マネージャにより、F-Secure 管理エージェントと選択された製品がホストにインストールされます。インストール時には、実行中の処理がステータス ラインに表示されます。[**キャンセル**] ボタンをクリックすることで、いつでもインストールを中止できます。

   ステータス ラインに「完了」と表示されると、インストールが完了します。[インポート] の設定を使用して、新しいホストを保存するドメインを選択できます。[**完了**] をクリックします。F-Secure ポリシー マネージャ コンソールは、このダイアログで別のドメインを指定しない限り、手順 1 で選択したドメインに新しいホストを保存します。また、ドメインに自動的にホストを保存しないように選択することもできます。新しいホストから自動登録情報を送信し、それに従ってホストをインポートできます。

7. 数分後、[製品ビュー] ウィンドウ（右側のウィンドウ）に、インストールされた製品のリストが表示されます。このリストを参照するには、[プロパティ] ウィンドウで [インストール] タブを選択します（または、[ポリシー ドメイン] ウィンドウで最上位ドメインを選択します）。

インストールが失敗する場合は、『FSII リモート インストールのエラー コード』(P229) で、最も一般的なエラー状況の説明を参照してください。

6.5.2 ポリシー ベース インストール

ベース ポリシー ファイルは、F-Secure 管理エージェントがインストールされているホストでインストールを開始するために使用されます。F-Secure ポリシー マネージャ コンソールは操作を指定したインストール パッケージを作成し、F-Secure ポリシー マネージャ サーバに格納して、ベース ポリシー ファイルにインストール タスクを書き込みます（このため、インストールの開始にはポリシー配布が必要です）。ベース ポリシー ファイルおよびインストール パッケージはいずれも、ホストが本物の情報だけを受け付けるように、管理用鍵ペアによって署名されます。

ホスト上の F-Secure 管理エージェントは F-Secure ポリシー マネージャ サーバから新しいポリシーを取り出し、インストール タスクを検出します。F-Secure 管理エージェントは、タスク パラメータで指定されたインストール パッケージをサーバから取り出して、インストール プログラムを開始します。

インストールが完了すると、F-Secure 管理エージェントはインクレメンタル ポリシー ファイルでインストール操作の結果をサーバに送信します。F-Secure ポリシー マネージャ コンソールは新しいステータス情報を検出し、結果を表示します。

アンインストールには、これらと同じ通信メカニズムが使用されます。

インストール エディタの使用

インストール エディタは、F-Secure 管理エージェントがインストールされているホストで使用する必要があります。インストール エディタにアクセスするには、[プロパティ] ウィンドウで [ポリシー] タブを開き、ルート ノード (F-Secure] サブツリー) を選択します。または、[プロパティ] ウィンドウで [インストール] タブを開きます。インストール エディタが [製品ビュー] ウィンドウに表示されます。

インストール エディタでは、現在選択しているホストまたはポリシー ドメインにインストールする製品を、管理者が選択します。

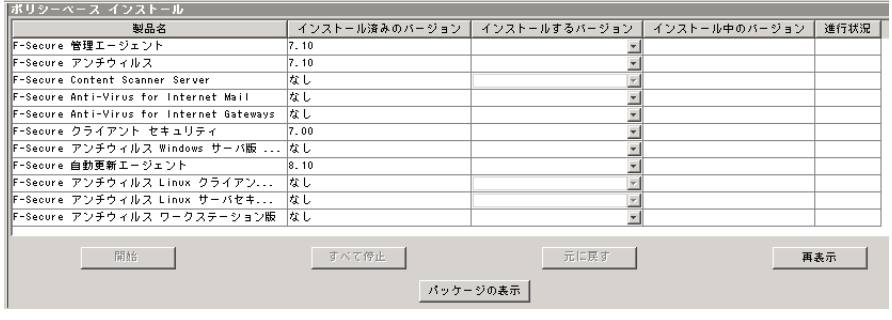


図 6-19 インストール エディタ

インストール エディタには、ポリシー ドメインまたはホストにインストールされる製品について以下の情報が表示されます。

製品名	ホストまたはドメインにインストールされる、または既存のインストール パッケージを使用してインストールできる製品の名前。
インストール済みのバージョン	製品のバージョン番号。製品の複数のバージョンがインストールされている場合、すべてのバージョン番号が表示されます。ホストの場合、バージョン番号は必ず 1 つです。

インストールするバージョン	製品のインストール パッケージのバージョン番号。
インストール中のバージョン	ホストまたはドメインにインストール中の現在のバージョン。
進行状況	インストール タスクの進行状況。[進行状況] フィールドに表示される情報は、ホストとドメインでは異なります。

ホストを選択している場合、[進行状況] フィールドには以下のいずれかのメッセージが表示されます。

進行中	インストール操作が開始（ポリシー データに追加）されましたが、インストールが成功したかどうかはホストから報告されていません。
失敗	インストールまたはアンインストールが失敗しました。[進行状況] フィールドのボタンをクリックして、詳細なステータス情報を参照してください。
完了	インストールまたはアンインストールが成功しました。インストール エディタを終了すると、このメッセージは消えます。
フィールドに何も表示されていない場合	実行中の操作はありません。[インストール済みのバージョン] フィールドに現在インストールされている製品バージョンが表示されます。

ドメインを選択した場合、[進行状況] フィールドには、以下のいずれかのメッセージが表示されます。

残りのホスト：<数>	<数> 個のインストールが失敗しました。残りのホストの数および失敗したインストールの数。[進行状況] フィールドのボタンをクリックして、詳細なステータス情報を参照してください。
完了	すべてのホストでインストールまたはアンインストールが成功しました。
フィールドに何も表示されていない場合	実行中の操作はありません。[インストール済みのバージョン] フィールドに現在インストールされている製品バージョンがすべて表示されます。

必要なバージョン番号をすべて選択したら、[**開始**] をクリックします。インストール エディタによって、インストール ウィザードが起動されます。このウィザードに従って、ユーザはインストールのパラメータを指定します。次にインストール エディタは、特定のインストール操作用にカスタマイズされた配布インストール パッケージを用意します。新しいパッケージは、F-Secure ポリシー マネージャ サーバに保存されます。

[**開始**] ボタンは、[インストールするバージョン] フィールドで選択したインストール操作の開始に使用します。最初に [**開始**] ボタンをクリックせずにインストール エディタを終了すると、変更はすべて破棄されます。

インストール操作ではポリシーベースのトリガが使用されるため、ユーザは新しいポリシー ファイルを配布する必要があります。ポリシー ファイルには、インストール パッケージを取り出して、インストールを実行するようホストに通知するエントリが追加されます。

インストール操作の実行には、かなり時間がかかることがあります。特に、操作対象のホストが現在ネットワークに接続されていない場合、または実行中のインストール操作で、ユーザがインストール完了前にホストを再起動するよう要求された場合は、時間がかかる可能性があります。ホストがネットワークに接続され、ポリシー ファイルを正常に送受信しているにもかかわらず時間がかかる場合は、実際に問題が発生し

ている可能性があります。また、ホストでインストール操作が正常に認識されていない可能性もあります。いずれの場合も、[すべて停止] をクリックすると、ポリシーからインストール操作を削除できます。これにより、選択したポリシー ドメインまたはホストに対して定義されたインストール操作はキャンセルされます。確認ダイアログで [サブドメインおよびホストのインストールを再帰的にキャンセル] オプションを選択すると、選択されたドメインおよびすべてのサブドメインでインストール タスクをすべて停止できます。

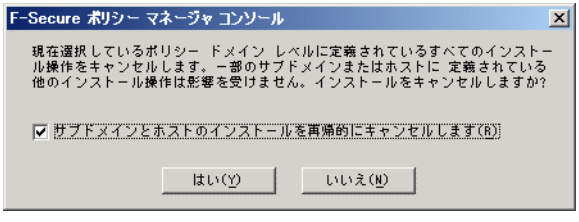


図 6-20 インストールのキャンセルの確認ダイアログ

[すべて停止] ボタンは、現在のホストまたはドメインにインストール操作が定義されている場合にのみ有効です。サブドメインの操作は、ボタンの状態に影響を与えません。[すべて停止] ボタンでは、ポリシーから操作が削除されるだけです。ホストがすでに前のポリシー ファイルをポーリングしている場合、インストール操作がインストール エディタに表示されなくなっても、そのホストではインストール操作が試行されます。

リモート アンインストール

アンインストールは、更新と同じように簡単に実行できます。製品のアンインストールに必要なソフトウェアのみが含まれた配布パッケージが作成されます。リモート アンインストールをサポートしていない製品の場合、インストール エディタにはアンインストールのオプションが表示されません。

[再インストール] を選択すると、現在のバージョンを再インストールします。このオプションは、問題を解決する場合のみ使用してください。通常、製品を再インストールする必要はありません。

F-Secure 管理エージェント

F-Secure 管理エージェントをアンインストールすると、F-Secure 管理エージェントが削除されて情報を送信することができないため、アンインストールが正常に完了したことを知らせる統計情報は送信されません。

たとえば、F-Secure アンチウィルスと F-Secure 管理エージェントをアンインストールする場合は、次の手順に従います。

1. F-Secure アンチウィルスをアンインストールします。
2. アンインストールが成功したかどうかが F-Secure ポリシー マネージャ コンソールから報告されるまで待ちます。
3. F-Secure アンチウィルスが正常にアンインストールされた場合は、F-Secure 管理エージェントをアンインストールします。
4. F-Secure 管理エージェントのアンインストールに失敗した場合は、F-Secure ポリシー マネージャ コンソールに、アンインストールが失敗したことを示す統計レポートが表示されます。正常なアンインストールは報告されませんが、切断された通信が認識され、F-Secure 管理エージェントの最終レポートに「進行中」と表示されます。

6.5.3 設定済みのパッケージを使用したローカル インストールおよび更新

設定済みのパッケージを、JAR または MSI (Microsoft Installer) 形式でエキスポートできます。MSI パッケージは、Active Directory 環境の Windows グループ ポリシーなどを使用して配布することができます。

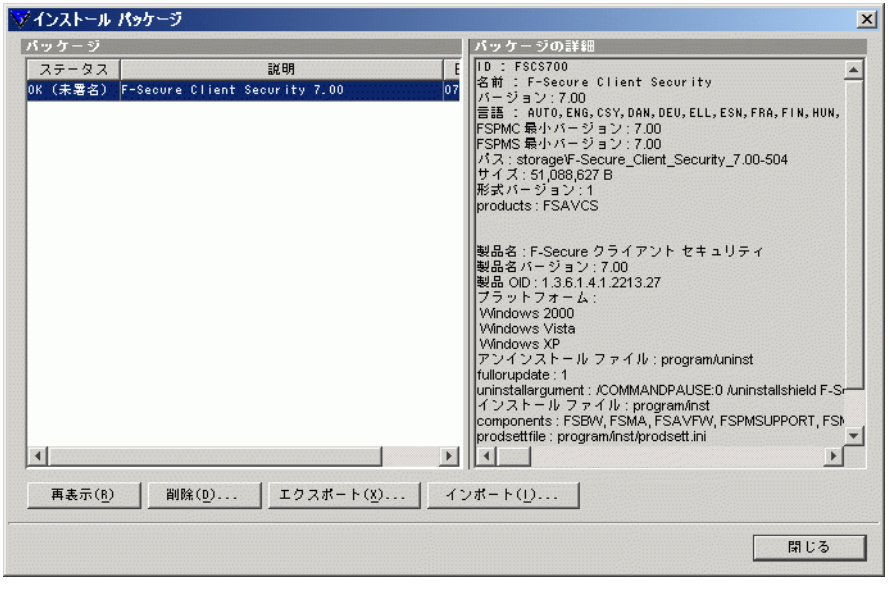
以下で説明するように、どちらの形式でエキスポートする場合も手順は同じです。[インストール パッケージのエキスポート] ダイアログで、カスタマイズしたパッケージのファイル形式を選択できます（手順 4 を参照）。

Windows プラットフォームでのログイン スクリプト

これを実行するには、カスタマイズしたリモート インストール JAR パッケージ、カスタマイズした MSI パッケージ、または JAR 以外の方法の 3 つの方法があります。

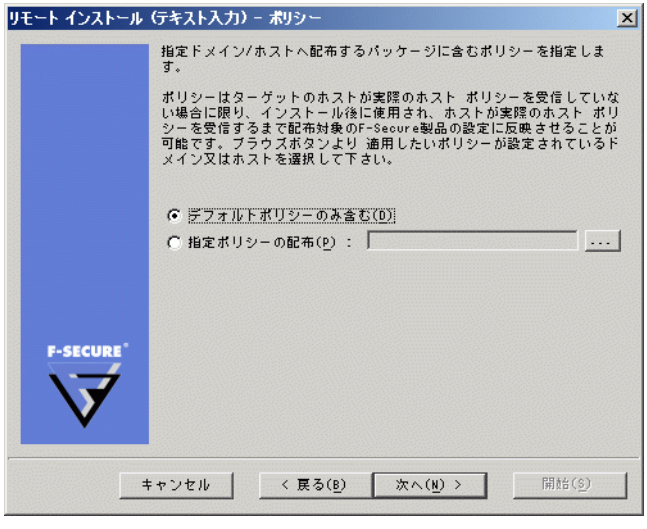
カスタマイズしたリモート インストール JAR パッケージの使用

1. F-Secure ポリシー マネージャ コンソールを実行します。
2. [ツール] メニューから [インストール パッケージ] を選択します。[インストール パッケージ] ダイアログ ボックスが表示されます。

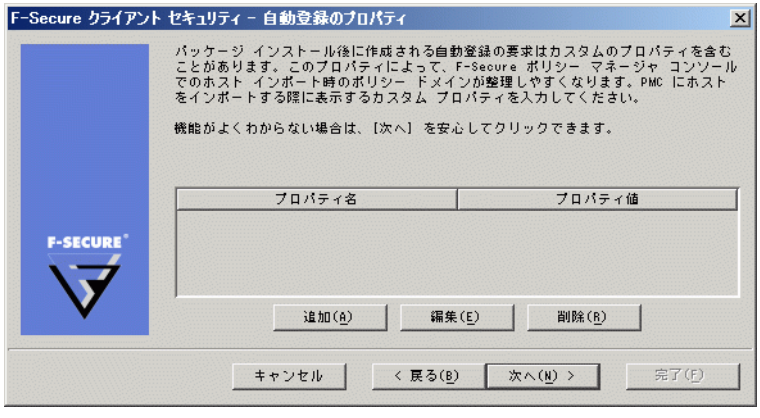


3. JAR または MSI のファイル形式と、カスタマイズしたインストール パッケージを保存する場所を指定します。[**エキスポート**] をクリックします。
4. カスタマイズしたインストール JAR パッケージを保存する場所を指定します。[**保存**] をクリックします。

5. インストールする製品を選択します（デフォルトでは、F-Secure 管理エージェントがインストールされます）。[次へ] をクリックして次へ進みます。
6. デフォルト ポリシーの使用を選択するか、匿名ポリシーとして使用する必要があるホストまたはドメイン ポリシーを指定します。[次へ] をクリックして次へ進みます。



7. インストールの方法を選択します。デフォルトの集中管理インストールを推奨します。
   また、スタンドアロンのホスト用にパッケージを準備することもできます。
8. インストール パッケージにはカスタム自動登録プロパティを必要な数だけ入れることができます。これらのカスタム プロパティは、ホストによって、ローカル インストールの後で F-Secure ポリシー マネージャに送信する自動登録メッセージに追加されます。これらのカスタム プロパティは標準ホスト識別プロパティとあわせて [自動登録] ビューに表示されます（『自動登録ホスト』(P106) を参照してください）。カスタム プロパティ名が列の名前となり、値がセルの値として表示されます。



カスタム プロパティの使用方法の例として、ユニット固有のポリシー ドメイン下でグループ化する必要があるさまざまな組織ユニットに対して、個別のインストール パッケージを作成する方法があります。プロパティ名はユニットとなり、値はインストール パッケージごとに異なります。これで、各ユニットからのホストを［自動登録］ビューで識別して、列の並べ替えおよび複数選択を使用して、1 つのユニットでのすべてのホストをインストール先ドメインにインポートできます。インストール先ドメインを［自動登録］ビューから直接変更した後、別のユニットからのホストをそのインストール先ドメインにインポートできます。

9. 概要ページにインストールの選択肢が表示されます。概要を確認し、［**開始**］をクリックしてインストール ウィザードを続行します。
10. F-Secure ポリシー マネージャ コンソールは、選択した製品のセットアップに必要なすべての情報を収集するリモート インストール ウィザードを表示します。

    ウィザードの最後のページで、［**完了**］をクリックして続行します。
11. エキスポートした JAR は、ilaunchr.exe ツールを実行してホストにインストールすることができます。ilaunchr.exe ツールは、ポリシー マネージャ コンソールのインストール先ディレクトリの ...¥Administrator¥Bin ディレクトリ以下に格納されています。以下の手順を実行してください。
    a. ilaunchr.exe とエキスポートした JAR を、ログイン スクリプトがアクセスできる場所にコピーします。
    b. 次のコマンドを入力します。

ilaunchr <パッケージ名>.jar

<パッケージ名> は、インストールしている JAR パッケージの名前で置き換えます。

インストールが実行されたら、インストールの進行状況を示すダイアログが表示されます。インストール後に再起動が必要な場合は、インストール パッケージのエキスポート時に定義したように、コンピュータを再起動するように指示が表示されます。

インストールをサイレント モードで実行する場合は、次のようにコマンドを入力します。

ilaunchr <パッケージ名>.jar /Q

この場合も、インストール後にコンピュータを再起動するように指示されます。インストール中に重大なエラーが発生した場合は、メッセージが表示されます。

ILAUNCHR では、以下のコマンドライン パラメータを指定できます。

/U ユーザ介入なし。重大なエラーが発生した場合でもメッセージが表示されません。

/F 強制的にインストールを実行します。F-Secure 管理エージェントがすでにインストールされている場合でも、インストールを実行します。

詳細なヘルプ情報を表示するには、コマンドラインで「ILAUNCHR /?」と入力します。終了エラー コードの一覧と、バッチ ファイルで使用可能な例については、『*ïtò^ B.* Ilaunchr のエラー コード』を参照してください。

JAR 以外の方法

1. 適切なインストール ファイルをインストール先ディレクトリにコピーします。インストール ファイルは CD-ROM の ¥software¥<アプリケーション>¥ ディレクトリにあります（たとえば、F-Secure クライアント セキュリティ 6.0 のファイルは、¥software¥fsavcs¥ にあります）。
2. 上記と同じインストール先ディレクトリに、admin.pub ファイルをコピーします。

3. prodsett.ini ファイルを編集します。このファイルには、インストールするモジュールとワークステーション上のインストール先（ディレクトリ）が指定されています。これらの情報は、セットアップ プログラムで使用されます。Prodsett.ini ファイルの編集の詳細については、『F-Secure クライアント セキュリティ管理者用ガイド』の**付録**「Modifying PRODSETT.INI」を参照してください。
4. ログイン スクリプトに以下の行を追加します。

   setup.exe¥silent /checkFSMA

   パラメータ /checkFSMA を使用しなければ、runsetup.exe を実行するたびにインストールが実行されます。

6.5.4 情報の転送

インストール情報はすべて、F-Secure ポリシー マネージャ サーバを通じてファイルとして転送されます。インストール パッケージは、WinZip などで表示可能な JAR アーカイブとなっていますが、ポリシー ファイルおよび INI ファイルなどその他のタイプのファイルは、実際のインストール処理を実行するために使用されます。

F-Secure ポリシー マネージャ サーバへのインストール パッケージの転送

F-Secure ポリシー マネージャ コンソールでインストールを開始する前に、初期インストール パッケージを F-Secure ポリシー マネージャ サーバに転送する必要があります。インストール パッケージは、以下の場所にあります。

- インストール用 CD-ROM
- F-Secure の Web サイト

通常、新しいリモート インストール パッケージは CD-ROM からインストールされ、インストールされたパッケージは、F-Secure ポリシー マネージャ セットアップによって自動的にサーバに移動されます。リモート インストール パッケージを他の方法で入手した場合は、［インストール パッケージ］ビューの［**インポート**］ボタンをクリックして

インポートするか、または［インストール パッケージ］ダイアログからインポートできます。または、サーバの /Install/Entry サブディレクトリに手動でインストール パッケージをコピーすることもできます。

F-Secure ポリシー マネージャ コンソールは、新しいインストール パッケージの使用を許可する前に、パッケージが F-Secure Corporation の秘密鍵で署名されているかどうかを確認します。

6.6 ポリシーの管理

6.6.1 設定

設定を行うには、ポリシーのツリーを参照してポリシー変数の値を変更します。

ポリシー変数には、2 つのタイプがあります。1 つはサブツリーの下のリーフ ノード、もう 1 つはテーブルのセルです。すべての変数には、関連付けられたタイプがあります。値は［製品ビュー］ウィンドウで設定できます。ポリシー変数のタイプには、以下のものがあります。

- 整数 ：普通の整数
- 表示文字列 :7 ビットの ASCII 文字列
- IP アドレス :4 オクテットの IP アドレス
- カウンタ ：一定の値ずつ増える整数
- ゲージ ：ラップしない整数
- 時間刻み ：経過した時間の単位（1/100 秒単位で測定）
- オクテット文字列 :バイナリ データ（このタイプは UNICODE の文字列でも使用されます）
- OID: オブジェクト識別子
- 非透過 ：追加のデータ タイプを表すことができるバイナリ データ

ポリシー変数には、デフォルト値が定義されている場合があります。デフォルト値は、ルート ドメインよりも上位から継承されたような形で適用されます。つまり、最上位（ルート）ドメインが選択されていても、デフォルト値は継承される値のように扱われます。デフォルト値は、他の値と同じように上書きできます。

選択したポリシー ドメイン レベルの値は、以下のように色分けされます。

- 黒 – 選択したポリシー ドメイン レベルまたはホスト レベルで変更された値
- 灰色 – 継承された値
- 赤 – 無効な値
- くすんだ赤 – 継承された無効な値

6.6.2 制約

制約には、**アクセス制約**と**値制約**の 2 つの種類があります。

アクセス制約には、[確定] または [非表示] を指定できます。[確定] を指定すると、ポリシーが常に強制的に適用されます。つまり、ポリシー変数はローカル ホストのあらゆる値を上書きし、制約が [確定] に設定されている限り、エンドユーザは値を変更できません。[非表示] を指定すると、エンドユーザからは値が見えなくなります。[確定] 制約とは異なり、[非表示] 制約は管理対象のアプリケーションによって無視されることがあります。

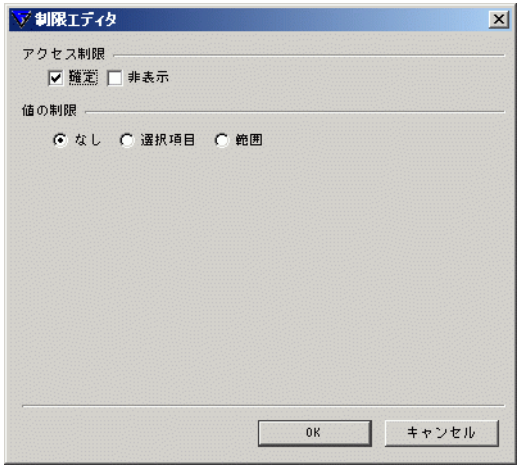


図 6-21 組み込み制約エディタ

値制約を使用することによって、管理者は、あらゆるポリシー変数の値をいくつかの値のリストに制限して、ユーザがその中から値を選択するようにすることができます。さらに、管理者は整数タイプの変数（整数、カウンタ、およびゲージ）の値の範囲を制限できます。追加の制約である［固定サイズ］制約は、テーブルに適用できます。この制約が適用されている場合、エンドユーザは固定サイズのテーブルに対して行を追加または削除できません。［確定］制約を空のテーブルに使用することはできません。空のテーブルには［固定サイズ］制約を使用します（エンドユーザがテーブルの値を変更できないようにします）。

製品の MIB の変数に範囲または選択できるオプションが定義済みである場合、管理者はこの範囲または選択できるオプションをさらに制限できます。ただし、範囲や選択できるオプションを増やすことはできません。製品の MIB で値制約が定義されていない場合、管理者は制約の範囲または選択できるオプションを指定できます。

制約は、組み込まれている［製品ビュー］ウィンドウ、または独立したダイアログ ボックスで編集できます。これらを切り換えるには、［表示］メニューから［組み込み制約エディタ］を選択します。組み込みエディタがオフになっている場合、［製品ビュー］ウィンドウにはダイアログ エディタを起動するためのボタンが表示されます。

6.6.3 現在のポリシー データの保存

ポリシー データは、ポリシー ドメイン構造、ドメインとホストのプロパティ、および各ポリシー ドメインとホストのポリシー情報が格納されたデータベースです。

ポリシー データを保存するには、[ファイル] メニューから [保存] または [名前を付けて保存] を選択します。ポリシー データに新しい名前を付けて保存し、必要に応じて古いポリシー設定に戻すことができるという理由から、[名前を付けて保存] をお勧めします。

6.6.4 ポリシー ファイルの配布

ドメインおよびホストの環境設定を完了したら、ホストに新しい環境設定を配布する必要があります。この操作を行うには、ツールバーの をクリックするか、[ファイル] メニューから [配布] を選択します（または CTRL+D キーを押します）。F-Secure ポリシー マネージャ コンソールは、保存されているポリシー データからベース ポリシー ファイルを生成します。ポリシー ファイルは通信ディレクトリにコピーされます。ホスト上の F-Secure ソフトウェアはこの通信ディレクトリを定期的にチェックします。ポリシー データとポリシー ファイルの違いを理解しておくことは重要です。ポリシー データは、ポリシー ドメイン構造全体が格納されたコンパクトなデータ構造体です。ベース ポリシー ファイルは、ポリシーを転送するためにポリシー配布時に生成されます。

ポリシー ファイルを配布して、ホストがそのファイルを取り出すまで、変更は反映されません。操作はポリシー ベースのメカニズムを使用して実装されているため、このことは操作にも当てはまります。

6.6.5 ポリシーの継承

F-Secure ポリシー マネージャ コンソールでは、各ポリシー ドメインが自動的に親ドメインの設定を継承します。それによって大規模なネットワークの管理が容易に効率よくできるようになります。継承された設定は、ホストやドメイン単位で上書きできます。ドメインの継承された

設定が変更された場合、変更内容はすべてのドメインのホストおよびサブドメインで継承されます。すべての設定は、［ 消去 ］ 操作で削除できます。設定は現在選択されているポリシー ドメインまたはホストから削除されるため、設定は親ドメインの設定で置き換えられます。

ポリシーの継承により、簡単に共通のポリシーを定義できます。サブドメイン、または個々のホストについて、ポリシーをさらに細かく定義できます。ポリシー定義をどこまで詳細に設定するかは、システムによりかなり開きがあります。大規模なドメインに少数の異なるポリシーを定義することもできれば、個々のホストに直接ポリシーを適用して、非常に細かい管理を実現することもできます。

このような計画を組み合わせることにより、最良の結果が得られます。一部の製品では大規模なドメインからポリシーを継承し、他の製品ではサブドメインからポリシーを継承するか、ホスト固有のポリシーを取得するということが可能です。

ポリシー ドメイン階層の複数のレベルでポリシーが変更されている場合、変更の追跡は非常に困難な作業になることがあります。特定のポリシー設定に加えられた変更を確認する場合、［ ドメインの値を表示 ］ 操作を使用すると便利です。

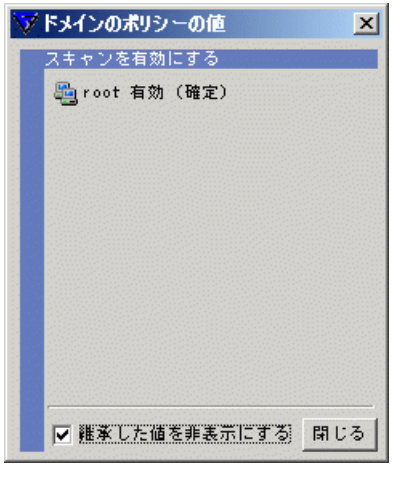


図 6-22 ［ ドメインの値を表示 ］ ダイアログ

サブドメインまたはホストの値を現在のドメインの値にリセットする必要がある場合は、[強制的に値を適用] 操作を使用して、サブドメインやホストの値を消去できます。

テーブルでのインデックスの継承

[**行を消去**] ボタンを使用してテーブルの行を消去すると、選択した行は空になります。選択した行を空にした後の結果は、親ドメインと MIB でデフォルトの行として定義されているデフォルト行の種類によって異なります。

- 消去した行と同じインデックス値を持つ行が存在する場合は、この行が再継承されます。
- 消去した行と同じインデックス値を持つ行が存在しない場合、[**行を消去**] 操作を実行した後は、この行は空のままになります。

行は親ドメインまたは MIB（設定の定義と、すべての設定デフォルト値が含まれています）からデフォルト行として継承できます。リーフ値や行の継承に関しては、MIB は「ルート ドメインより上位のドメイン」とみなすことができます。MIB のデフォルトは、ドメイン レベルで上書きしない限り、サブドメインに継承されます。継承された行を上書きする場合は、同じインデックス列値を持つ行を定義します。

一部の F-Secure 製品はデフォルトのテーブル実装を上書きします。つまり、これらの製品は、上記のような通常のテーブル継承を実装していません。

たとえば、次のテーブルでは、基本的なテーブル継承はなく、独自のメカニズムが使用されます。

- F-Secure インターネット防御の [ルール] テーブル
- F-Secure インターネット防御の [サービス] テーブル
- F-Secure VPN+ の [接続] テーブル

このような場合のテーブルの動作の詳細については、対応する製品のマニュアルを参照してください。

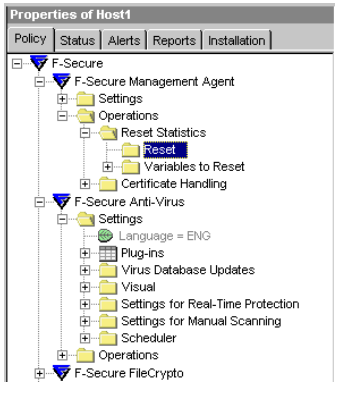
継承された行とローカルで派生された行は色で区別できます。継承された行は灰色、ローカルで派生された行は黒で表示されます。

6.7 操作とタスクの管理

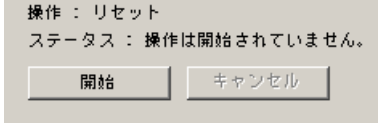
6.7.1 操作

F-Secure ポリシー マネージャ コンソールから操作を開始するには、次の手順に従います。

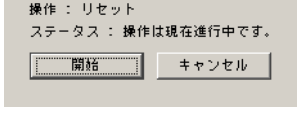
1. ［プロパティ］ウィンドウの［ポリシー］タブで、選択した製品の［操作］ブランチを選択し、いずれかの処理を選択します。



2. ［製品ビュー］ウィンドウに次のウィンドウが表示されます。［開始］をクリックして、選択した操作を開始します。



3. 新しいポリシーを配布して、ホストがそのポリシー ファイルを取り出すと、直ちに操作がホスト上で開始されます。［キャンセル］ボタンをクリックすると、いつでも操作を中止できます。



6.8 警告の送信

6.8.1 警告とレポートの表示

プログラムまたは操作に問題がある場合、ホストは警告とレポートを送信できます。警告を受信すると、 ボタンが強調表示されます。警告を表示するには、 をクリックします。[プロパティ] ウィンドウの [警告] タブが表示されます。受信した警告はすべて、以下の形式で表示されます。

	確認	警告を確認するには、[**確認**] ボタンをクリックします。すべての警告を確認すると、[**確認**] ボタンが淡色表示されます。
	深刻度	問題の重大度。以下のアイコンで、重大度を示します。
	情報	ホストからの通常の操作情報
	警告	ホストからの警告です。
	エラー	ホスト上の回復可能なエラーです。
	重大なエラー	ホスト上の回復不能なエラー
	セキュリティ警告	ホスト上のセキュリティ危険要因
	日付 / 時間	警告の日付と時刻。

概要	問題の説明。
ホスト / ユーザ	ホストまたはユーザの名前。
製品	警告の送信元の F-Secure 製品。

リストから警告を選択すると、[製品ビュー] ウィンドウに警告の詳細情報が表示されます。F-Secure アンチウィルスのスキャン警告には、レポートが添付されている場合があります。このレポートも、[製品ビュー] ウィンドウに表示されます。

レポートを表示するには、[プロパティ] ウィンドウの [レポート] タブをクリックするか、[製品ビュー] メニューから [メッセージ] を選択します。[レポート] タブは、[警告] タブと同じ構造になっています。

列の見出しをクリックすると、[警告] テーブルと [レポート] テーブルをソートできます。

6.8.2 警告転送の設定

[警告の転送] テーブルを編集して、警告を設定することができます。このテーブルは、[F-Secure 管理エージェント] -> [設定] -> [警告] -> [警告の転送] にあります。

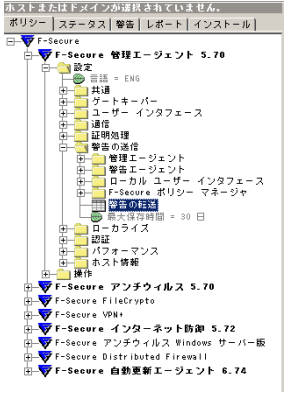


図 6-23 [F-Secure 管理エージェント] > [設定] > [警告の転送]

このテーブルは［警告の転送］タブにある F-Secure 管理エージェントの製品ビューでも参照できます。

セキュリティ レベルに応じて、警告の送信先を指定できます。F-Secure ポリシー マネージャ コンソール、ローカル ユーザのインタフェース、警告エージェント（イベント ビューア、ログ ファイル、SMTP など）、または管理エクステンションを指定できます。

［警告の転送］テーブルにはデフォルト値が設定されています。

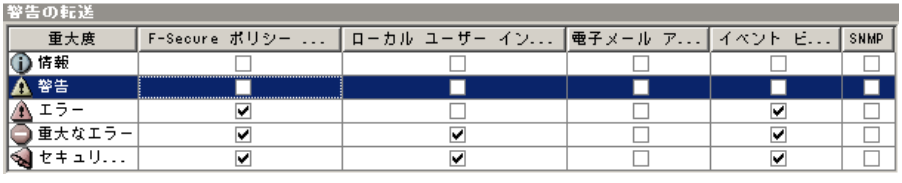


図 6-24［警告転送］テーブル

デフォルトでは、情報の警告とワーニング レベルの警告は、F-Secure ポリシー マネージャ コンソールに送信されたり、ユーザに表示されたりしません。優先度が低い警告と通知は、問題の解決に非常に便利な情報です。ただし、これらの警告を有効にすると、転送される警告の数がかなり増加します。大規模なドメイン構造の場合、ルート ドメイン レベルで厳密な警告転送ルールを設定すると、大量の警告が F-Secure ポリシー マネージャ コンソールに送信される可能性があります。

送信先別のブランチでポリシー変数を設定して、警告の送信先をさらに詳細に設定できます。たとえば、［設定］->［警告］->［F-Secure ポリシー マネージャ コンソール］->［再送試行間隔］では、ホストから F-Secure ポリシー マネージャ コンソールへの警告の送信が失敗した場合に、次に再試行するまでの間隔を指定します。

6.9 レポート ツール

レポート ツールを使用すると、F-Secure ポリシー マネージャ コンソールで管理されているデータのレポートを表示したり、エキスポートすることができます。表示およびエキスポートの機能により、複数のホストやドメインのデータを同時に効果的に確認できます。

レポート ツールを起動するには、[ツール] メニューから [レポート] を選択します。F-Secure ポリシー マネージャ コンソールの [ポリシー ドメイン] ウィンドウのコンテキスト メニューからも、レポート ツールを起動することができます。

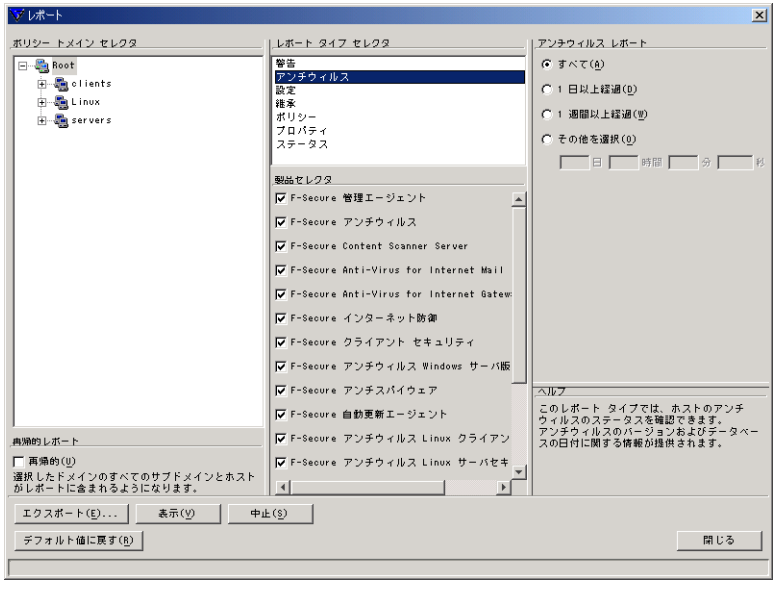


図 6-25 レポート ツール

6.9.1 [ポリシー ドメイン / ホスト セレクタ] ウィンドウ

[ポリシー ドメイン / ホスト セレクタ] ウィンドウでは、レポートの対象とするドメインやホストを選択できます。レポート ツールでは、[ポリシー ドメイン] ウィンドウで選択されているドメインがデフォルトで選択されます。

[再帰的] チェックボックスをオンにすると、ドメイン階層の選択されたドメイン内に再帰的に入るすべてのホストもレポートに含まれます。

6.9.2 ［レポート タイプ セレクタ］ウィンドウ

［レポート タイプ セレクタ］ウィンドウでは、以下の操作を実行できます。

- 作成するレポート タイプの選択
- 製品別のフィルタリング（作成されるレポートには、選択した製品の情報だけが含まれるようになります）

現在選択可能なレポート タイプは次のとおりです。

［ポリシー］レポート タイプ	選択したドメイン コンポーネントで選択した製品の、すべてのポリシー変数を含んでいるレポートをエキスポート / 表示します。同時に［継承］チェッ クボックスをオンにして、レポートに継承情報を含めることもできます。
［継承］レポート タイプ	選択したドメイン コンポーネントで選択した製品の、上位レベルのドメインから継承されていないすべてのポリシー変数（つまり、選択したドメイン コンポーネントで定義されているすべてのポリシー変数）の値を含んでいるレポートをエキスポート / 表示します。
［ステータス］レポート タイプ	選択したドメイン コンポーネントで選択した製品の、すべてのローカル設定とステータス変数を含んでいるレポートをエキスポート / 表示します。
［プロパティ］レポート タイプ	ドメイン コンポーネントのすべてのプロパティ フィールドの値を含んでいるレポートをエキスポート / 表示します。また、［プロパティ セレクタ］チェックボックスを使用して、作成するレポートに含めるプロパティ フィールドを選択することもできます。

［警告］レポート タイプ	選択したドメイン コンポーネントのすべての警告情報を含んでいるレポートをエキスポート / 表示します。また、［ソート順セレクタ］を使用して、警告の説明フィールド間でソート順を定義して、警告をソートすることもできます。［重大度セレクタ］を使用すると、作成するレポートに含める警告の重大度を選択できます。
［設定］レポート タイプ	選択したドメイン コンポーネントで選択した製品の、インストールされている製品の情報を含んでいるレポートをエキスポート / 表示します。
［アンチウィルス］レポート タイプ	アンチウィルスのバージョンと更新パターン ファイルのドメイン コンポーネント ステータスを含んでいるレポートをエキスポート / 表示します。

6.9.3 ［レポート］ウィンドウ

［レポート］ウィンドウでは、次の操作を行うことができます。

- 現在選択しているレポート タイプに対応する設定の選択。レポート タイプに対応する設定を使用して、作成するレポートのフィルタリングをさらに調整できます。
- 現在選択しているレポート タイプの説明の検索。

現在選択可能なレポート タイプの設定には、次のものがあります。

- ポリシー レポート タイプに対応する設定 - 作成するレポートに含めるポリシー値の継承情報を選択できます。
- プロパティ レポート タイプに対応する設定 - ID、プラットフォーム、その他、および VPN+ プロパティのどの情報を作成するレポートに含めるかを選択できます。
- 警告 レポート タイプに対応する設定 - すべての警告説明フィールドで警告をソートしたり、作成するレポートに含める警告の重要度によって警告を選択したりできます。

6.9.4 下部のウィンドウ

下部のウィンドウでは、次の操作を行うことができます。

- すべてのユーザ インタフェース コンポーネントをデフォルトに戻す。
- レポートのエキスポート処理を起動する。
- レポートの表示処理を起動する。
- レポートの生成処理を停止する。
- レポート ツールのユーザ インタフェースを終了する。これによってエキスポートするレポートの生成が終了することはありません。レポートの生成は、バックグラウンドで実行されます。表示目的のレポート生成は、表示されるダイアログで停止できます。

レポートの表示

選択したレポート タイプのレポートを選択した設定で生成するには、下部のウィンドウで［**表示**］をクリックします。その後、レポートはデフォルトの Web ブラウザで HTML 形式で表示できます。デフォルトの Web ブラウザが定義されていない場合、Web ブラウザを定義するようダイアログ ボックスが表示されます。

レポートのエキスポート

選択したレポート タイプのレポートを選択した設定で生成するには、下部のウィンドウで［**エキスポート**］をクリックします。作成するレポートのパスとレポート形式は、表示される［ファイルの保存］ダイアログで定義できます。その後、レポートは、選択したファイルに選択したレポート形式でエキスポートされます。

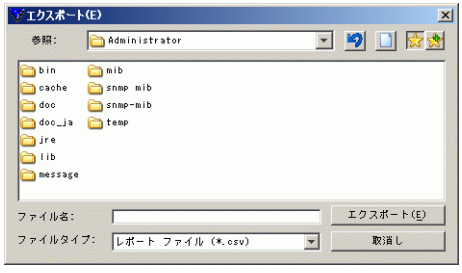


図 6-26 レポートの保存とエキスポート

6.10 一般設定

［一般設定］の設定は、すべての接続で共有されるか、または特定の接続に適用されます。

6.10.1 接続固有の一般設定

これらの設定を編集するには、[ツール] メニューから [一般設定] を選択します。現在の接続オブジェクトだけが影響を受けます。

タブ	設定	意味
通信	ポーリング間隔	異なるパッケージ タイプのポーリング間隔。チェックボックスをオンまたはオフにして、特定のパッケージ タイプのポーリングを有効または無効にできます。常に自動ポーリングの代わりに手動更新の操作を実行する場合は、[すべてのポーリングを無効にする] チェックボックスをオンにします。
	ホストの接続ステータス	ホストが F-Secure ポリシー マネージャから切断されたと見なされる時間を設定します。定義した時間 F-Secure ポリシー マネージャ サーバにアクセスしていないホストは、すべて切断されたものと判断されます。切断されたホストのドメイン ツリーには通知アイコンが表示されます。さらに、これらのホストは [ドメインのステータス] ビューの [接続を切断されたホスト] リストに表示されます。ドメイン ツリーに通知アイコンを表示するかどうかは、[**詳細オプション**] で切り替えることができます。1 日未満の間隔を定義するには、設定フィールドに浮動小数点型の数値を入力します。たとえば、「0.5」に設定すると、12 時間以内にサーバに接続しなかったホストはすべて切断されたものと見なされます。通常の環境では一部のホストが時々サーバから自然に切断されるため、1 日未満の値は通常、トラブルシューティングのために使用する場合のみに役立ちます。たとえば、ノート型コンピュータはサーバに毎日アクセスできない可能性がありますが、通常はこれは正常な現象です。
通信の詳細オプション	ステータスのキャッシュ	F-Secure ポリシー マネージャ コンソールがステータス情報をキャッシュするホストの数を調整できます。

初期ステータスのロードを無効にする	大規模な環境で F-Secure ポリシー マネージャ コンソールの起動時間を短縮する場合は、ステータスの初回のロードを無効にします。これは高度なオプションで、通常のステータス処理に次のような違いが生じるため、注意して使用する必要があります。 1. どのホストにもソフトウェアがインストールされていないものと見なされます。これは［プロパティ］ウィンドウとインストール エディタに影響します。 2. 初期状態ではステータス項目を使用できなくなります。これは、［ステータス］タブを選択している場合に、［プロパティ］ウィンドウと製品ビューに影響します。 3. MIB バージョン情報が使用できなくなるため、すべてのホストは最新の MIB バージョンから生成されたポリシーを受け取ります。 ステータスの初回のロードをスキップしても、手動でのステータスの再表示や定期的なステータス ポーリングには影響がありません。必要に応じて、ステータスの自動ポーリングを無効にできます。このためには、［ツール］メニューから［一般設定］を選択します。続いて、［通信］タブを選択して［**ポーリング間隔オプション**］をクリックし、［すべてのポーリングを無効にする］チェックボックスをオンにします。 初回のステータス ポーリングをスキップにするには、次のいずれかの方法を使用できます。 ■ Administrator.properties 環境設定ファイルを使用して、デフォルト プロパティ「fsa.status.initialStatusLoading.on=true」を「fsa.status.initialStatusLoading.on=false」に変更する。 ■ Administrator.properties ファイルの接続固有設定を使用して、特定の接続エントリに対してステータスの初回のロードを無効にする。このためには、プロパティと値のペア「fsa.status.initialStatusLoading.on.<fsms?>=true」を追加します。

	バックグラウンドでの警告のロード	バックグラウンドでのロードを有効にすると、警告ビューを開いていない場合も警告がサーバからダウンロードされます。場合によっては、これにより警告ビューの表示速度が速くなることがありますが、F-Secure ポリシー マネージャ コンソールと F-Secure ポリシー マネージャ サーバの間で無駄なネットワーク トラフィックが大量に発生する可能性があります。
	バックグラウンドでのレポートのロード	「バックグラウンドでの警告のロード」を参照してください。
ポリシー ファイル	ポリシー ファイルの最適化	[**インデント**] - ファイルを作成する際に、人間が認識しやすいようにファイルに区切り文字を追加するかどうかを定義します。[インデント] をオフに切り替えると、区切り文字は追加されません。人間にとっては認識しにくくなりますが、データは完全に正しく、マシンによる認識に問題はありません。区切り文字としてスペースまたはタブを選択できます。スペースよりもタブを使用した方がファイル サイズが小さくなるので、タブをお勧めします。 [**コメントを入れる**] - F-Secure ポリシー マネージャ コンソールが作成するポリシー ファイルのサイズに影響します。コメントを使用すると、ユーザが直接ファイルから値を読み取る場合にファイルの内容を理解しやすくなります。 一般的にこれらの設定はデバッグ時にのみ使用され、通常の運用時には、インデントとコメントの両方を無効にしておいてもかまいません。
	ポリシー ファイルのシリアル番号	生成したベース ポリシー ファイルのシリアル ファイル。シリアル番号は自動的に増加していきます。通常、これは手動で調整する必要はありません。シリアル番号の値が小さいためにポリシー ファイルをホストが受け付けない場合、値を増加するだけで済みます（ホストはこのエラーを報告します）。この場合、シリアル番号は、ホストによって取得された最新のベース ポリシー内のシリアル番号よりも大きくなるように増加させる必要があります。

インストール情報の送信	インストールのタイムアウト	インストール情報の送信時にインストール操作を実行できる最大時間です。 **注** ：リモート インストール時にはエンドユーザに対して進行状況インジケータが表示されます。
	ブラウズ タイムアウト	[すでに管理対象のホストを非表示] オプションを使用している場合にのみ重要です。これは、ホストのレジストリにアクセスできる最大時間です。
	同時に行うネットワーク操作の最大数	ネットワーク操作の数を調整できます。デフォルト値をお勧めします。ただし、ネットワーク接続が低速で、インストール情報の送信時に問題が発生する場合は、接続速度に応じて同時ネットワーク接続の数を減らしてください。
	進行状況インジケータ	リモート インストール中にエンドユーザに対して進行状況インジケータを表示できます。

6.10.2 共有一般設定

これらの設定は、F-Secure ポリシー マネージャ コンソールの特定のインストールで定義されているすべての接続に適用されます。

タブ	設定	意味
[表示設定] -> [一般オプション]	言語	言語選択。オペレーティング システムのローカル言語、またはデフォルトの英語を選択できます。システムのローカル言語をサポートしていないすべてのオブジェクトは、英語で表示されます。変更を有効にするには、F-Secure ポリシー マネージャ コンソールを再起動する必要があります。
[表示設定] -> [ポリシー ドメイン]	切断されたホストを強調表示する	切断されたホストをポリシー ドメイン ツリーで強調表示できます。
	フォント	F-Secure ポリシー マネージャ コンソール全体で使用するフォントです。フォントの変更は、プログラムの再起動後に適用されます。

	ルック アンド フィール	ユーザ インタフェースのコンポーネントの外観と動作を定義します。変更は、プログラムの再起動後に適用されます。
ポリシー ファイル	製品	インストールされていない製品の MIB を非アクティブにし、配布するポリシー ファイルからこれらの MIB を除外できます。MIB を非アクティブにすると、管理対象ホストに送信されるポリシー ファイルのサイズが減少します。 **警告 : F-Secure から指示がない限り、MIB を非アクティブにしないでください。特定の管理対象ホストに実際にインストールされている製品の MIB を非アクティブにすると、システムの誤動作が発生する場合があります。**
インストール情報の送信	キャッシュの消去	ブラウズしたホストやインストール済みソフトウェアに関するすべてのキャッシュされた情報を消去して、ディスク領域を空けることができます。
所在地	Web Club の地域	最も近くにある F-Secure Web サーバに接続するための場所を選択します。
	HTML ブラウザのパス	HTML ブラウザの実行可能ファイルへのフル パスです。ブラウザは、オンライン ヘルプ ページ、Web Club ページ、およびアンチウィルス レポート ページを表示するのに使用されます。
	メッセージ ログのパス	[メッセージ ビュー] の各タブのログ ファイルが作成されるディレクトリへのパスを入力できます。各ログ ファイルには、対応するタブのタイトルと、重大度と作成時間を含むメッセージが 1 行あたり 1 つ含まれます。
	メッセージを保存	メッセージの保存のオン / オフを切り替えます。ログ情報はトラブルシューティングに役立つため、できるだけこの設定はオンにしておいてください。
アンチウィルス	パターン ファイル	この値を使用して、アンチウィルス モードでパターン ファイルを期限切れとみなすまでの経過時間を定義できます。

7 F-SECURE ポリシー マネージャ サーバのメンテナンス

概要 156
F-Secure ポリシー マネージャ コンソール データのバックアップと復元 156
イメージファイルを使用したソフトウェアの複製 159

7.1 概要

F-Secure ポリシー マネージャ サーバは、サーバ内のコンソール データを定期的にバックアップおよび復元することによってメンテナンスできます。

7.2 F-Secure ポリシー マネージャ コンソール データのバックアップと復元

重要な管理情報を定期的にバックアップすることは大事なことです。少なくても、通信ディレクトリの fsa¥domains ディレクトリ全体を定期的にバックアップすることを推奨します。通常、通信ディレクトリは、F-Secure ポリシー マネージャ サーバのインストール先ディレクトリの commdir¥ にあります。このディレクトリには、ポリシー ドメイン構造および保存されているすべてのポリシー データが格納されています。

fsa¥domains ディレクトリをバックアップする前に、F-Secure ポリシー マネージャ コンソールのセッションがどれも開いていないことを確認してください。

リポジトリ全体をバックアップすることもできます。リポジトリ全体をバックアップすることで、ポリシー ドメイン構造だけでなく、警告、ホストの統計、およびインストール操作も復元できるようになります。また、ポリシー ファイルもすばやく復元できるようになります。fsa¥domains ディレクトリのみをバックアップした場合は、後でポリシーを配布する必要があります。リポジトリ全体をバックアップする短所は、バックアップするデータが fsa¥domains ディレクトリ内のデータの数十倍になることです。また、全体のバックアップを実行する前に F-Secure ポリシー マネージャ サーバを停止しなければなりません。

管理用鍵ペアをバックアップするには、admin.prv と admin.pub を、ローカルの F-Secure ポリシー マネージャ コンソールのインストール先ディレクトリのルートからコピーします。admin.prv は、安全な場所に保管してください。admin.prv 鍵ファイルのバックアップ コピーを保存することは非常に重要です。

管理用鍵（admin.pub または admin.prv）を紛失した場合、ポリシー ベースの操作は使用できなくなるため、新しい鍵ペアを作成し、各ホストを手動で再インストールして、すべての管理対象ホストに各 admin.pub 鍵を配布する必要があります。F-Secure ポリシー マネージャ コンソールと管理されるホスト間の信頼は、電子署名に基づいています。適切な秘密鍵なしでは、ホストが受け付ける有効な署名を作成することはできません。

F-Secure ポリシー マネージャ コンソールの設定を保存する場合は、ローカルのインストール先ディレクトリから lib¥Administrator.properties ファイルをバックアップします。

Administrator.properties は、初めて F-Secure ポリシー マネージャ コンソールを実行したときに作成され、ウィンドウ サイズ、通信ディレクトリのパス、サーバの URL など、セッションに関連する情報を含んでいます。

バックアップの作成

バックアップを作成するには、次のいずれかの方法を選択できます。

- **フル バックアップ**
  ポリシー ドメインの構造、警告データ、ホストの統計およびインストール操作をバックアップして、復元することが可能です。
- **ポリシー データとドメイン構造のバックアップ**
  ポリシー マネージャ サーバのリポジトリ（Commdir）の fsa¥domains ディレクトリをバックアップします。

フル バックアップ

1. F-Secure ポリシー マネージャ コンソールの管理セッションをすべて閉じます。
2. F-Secure ポリシー マネージャ サーバのサービスを停止します。
3. 通信ディレクトリをバックアップします。

4. F-Secure ポリシー マネージャ コンソールのローカルのインストール先ディレクトリのルートにある admin.prv と admin.pub をバックアップします。
5. F-Secure ポリシー マネージャ コンソールのローカルのインストール先ディレクトリにある、lib¥Administrator.properties をバックアップします。
6. F-Secure ポリシー マネージャ サーバのサービスを再起動します。
7. F-Secure ポリシー マネージャ コンソールの管理セッションを再開します。
8. ポリシーを配布します。

ポリシー データとドメイン構造のバックアップ

1. F-Secure ポリシー マネージャ コンソールの管理セッションをすべて閉じます。
2. fsa¥domains ディレクトリをバックアップして、バックアップ コピーを安全な場所に保管します。
3. F-Secure ポリシー マネージャ コンソールの管理セッションを再開します。
4. ポリシーを配布します。

バックアップの復元

通信ディレクトリの全内容と、鍵や設定などのコンソール情報をバックアップした場合（フル バックアップ）、次の手順で復元します。

1. F-Secure ポリシー マネージャ コンソールの管理セッションをすべて閉じ、F-Secure ポリシー マネージャ サーバのサービスを停止します。
2. 通信ディレクトリを削除します。
3. 通信ディレクトリのバックアップを適切の場所にコピーします。
4. admin.pub を通信ディレクトリのルートおよびコンソールのインストール先ディレクトリのルートにコピーします。
5. admin.prv をコンソールのインストール先ディレクトリのルートにコピーします。
6. コンソールの設定（Administrator.properties）を＜コンソールのインストール先ディレクトリ＞\lib ディレクトリにコピーします。

7. F-Secure ポリシー マネージャ サーバのサービスを再起動します。
8. F-Secure ポリシー マネージャ コンソールの管理セッションを再開します。
9. ポリシーを配布します。
10. ポリシー ドメイン構造のみをバックアップした場合は（ポリシー データとドメイン構造のバックアップ）、次の手順で復元します。
11. F-Secure ポリシー マネージャ コンソールの管理セッションをすべて閉じ、F-Secure ポリシー マネージャ サーバのサービスを停止します。
12. <communication directory>¥fsa¥domains ディレクトリの内容を削除します。
13. バックアップしたデータを、上記と同じディレクトリにコピーします。
14. F-Secure ポリシー マネージャ サーバのサービスを再起動します。
15. F-Secure ポリシー マネージャ コンソールの管理セッションを再開します。
16. ポリシーを配布します。

7.3 イメージファイルを使用したソフトウェアの複製

ディスク イメージ ファイルを使用してソフトウェアを複製する場合、F-Secure アンチウィルスを含めることができます。ただし、インストールしたすべての製品には、F-Secure ポリシー マネージャで使用される固有の識別コード（固有の ID）が割り当てられます。ディスク イメージ ソフトウェアを使用して新しいコンピュータをインストールしようとすると、複数のコンピュータが同じ固有の ID を使用しようとする場合があります。このような状況になると、F-Secure ポリシー マネージャは正常に機能しなくなります。

次の手順に従って、ディスク イメージ ソフトウェアを使用した場合でも各コンピュータで専用の固有 ID が使用されるようにしてください。

1. イメージ ファイルに含める必要があるシステムとすべてのソフトウェアをインストールします（F-Secure アンチウィルスを含む）。正しい F-Secure ポリシー マネージャ サーバを使用するように F-Secure アンチウィルスを設定します。ただし、ホストが

F-Secure ポリシー マネージャ サーバに自動登録の要請を送信した場合、F-Secure ポリシー マネージャ コンソールにホストを**インポートしない**でください。インポートするのは、イメージ ファイルをインストールするホストのみにする必要があります。

2. コマンドプロンプトから fsmautil resetuid コマンドを実行します。通常、このユーティリティは C:¥Program Files¥F-Secure¥Common ディレクトリにあります（他言語の Windows を使用している場合、またはデフォルト以外のインストール パスを指定した場合は、ディレクトリのパスが違う場合があります）。
3. コンピュータをシャットダウンします。この時点で、コンピュータを**再起動しない**でください。
4. ディスク イメージ ファイルを作成します。
5. F-Secure アンチウィルス インストールの固有 ID は、ユーティリティ プログラムによってリセットされます。システムの再起動中に新しいユニーク ID が自動的に作成されます。この処理は、イメージ ファイルがインストールされた各マシン上で個別に実行されます。これらのマシンは F-Secure ポリシー マネージャに自動登録要求を送信し、要求を正常に処理できます。

8 F-SECURE パターンファイルの更新

F-Secure 自動更新エージェントによる自動更新 162
F-Secure ポリシー マネージャ プロキシによる自動更新 176

8.1 F-Secure 自動更新エージェントによる自動更新

F-Secure 自動更新エージェントを使用すると、他の作業を中断せずに、パターン ファイルと情報コンテンツを自動的に Web からダウンロードできます。F-Secure 自動更新エージェントでは、他のインターネット アプリケーションで使用されていない帯域幅を使用して、ファイルをバックグラウンドで自動的にダウンロードします。これによりユーザは、Web を検索しなくても常に最新版を入手できます。

F-Secure 自動更新エージェントがインターネットに常時接続されている場合、クライアントは新しい自動更新を、F-Secure が発行してから約 2 時間後に自動的に受け取ることができます。インターネットへの接続がいつ利用できるかによっては、これ以上時間がかかることもあります。

F-Secure 自動更新エージェントは、一元集中管理された、またはスタンドアロンの F-Secure 製品を更新するのに使用します。デフォルトで、ウィルス ニュースもダウンロードされます。必要に応じて、これらをダウンロードしないようにすることもできます。F-Secure 自動更新エージェントのインストールと使用には、ライセンス認証された F-Secure アンチウィルスやセキュリティ製品のインストールが必要です。

本製品の動作

F-Secure 自動更新エージェントはサービスを開始すると、F-Secure の自動更新サーバに接続します。エージェントは、サーバを定期的にポーリングして、新しいコンテンツが入手可能かどうかを確認します。新しいコンテンツが存在する場合は、それが自動的にダウンロードされます。ポーリング間隔はサーバ側で設定し、クライアント側からは調整できません。

F-Secure 自動更新エージェントと F-Secure ポリシー マネージャ サーバの通信には、HTTP プロトコルが使用されます。F-Secure 自動更新エージェントが F-Secure 更新サーバと通信するときに、デフォルトで UDP ベースのポライト プロトコルが使用されます。ポライト エージェント プロトコルを使用した場合、デフォルトでは、ネットワーク接続の未使用の帯域幅だけを使用してダウンロードが実行されます。つまり、ポライト プロトコルを使用したダウンロードは、他のインター

ネット接続に影響を与えません。クライアントが企業ファイアウォールの背後にインストールされている場合は、ポライト エージェント プロトコルの代わりに HTTP プロトコルを使用します。

F-Secure ポリシー マネージャ 6.0 以降では、F-Secure アンチウィルス製品と一緒にインストールされた自動更新エージェントが、設定された更新ソースから次の順序で自動更新のダウンロードを試みます。

a. 企業ネットワークでポリシー マネージャ プロキシが使用されている場合、クライアントはプロキシ マネージャ プロキシを順番に使用して F-Secure ポリシー マネージャ サーバに接続を試みます。
b. クライアントが HTTP プロキシを使用するように設定されている場合は、F-Secure ポリシー マネージャ サーバから HTTP プロキシを通して更新をダウンロードしようとします。
c. 続いて、クライアントは更新を F-Secure ポリシー マネージャ サーバから直接ダウンロードしようとします。
d. 企業ネットワークでポリシー マネージャ プロキシが使用されている場合、クライアントはプロキシ マネージャ プロキシを順番に使用して F-Secure 更新サーバに接続を試みます。
e. クライアントが HTTP プロキシを使用するように設定されている場合は、F-Secure 更新サーバから HTTP プロキシを通して更新をダウンロードしようとします。
f. 続いて、クライアントは更新を F-Secure 更新サーバから直接ダウンロードしようとします。

F-Secure 自動更新エージェントを使用する利点

パターン ファイルの更新の最適化されたダウンロード

F-Secure 自動更新エージェントは、パターン ファイルの変更を検出します。高度なバイトレベルのアルゴリズムを使用して、ファイル全体またはデータベース全体ではなく、変更された部分だけをダウンロードします。通常、変更部分は更新ファイルのほんの一部分であるため、低速モデムを使用しているダイヤルアップ接続のユーザは簡単に日々の更新を入手でき、常時接続しているユーザは帯域幅を大幅に節約できるようになります。

再開可能なデータ転送

F-Secure 自動更新エージェントでは、複数のセッションにまたがるダウンロードが可能です。ダウンロードが中断された場合、F-Secure 自動更新エージェントはダウンロードした内容を保存し、次回接続したときにファイルの残りをダウンロードします。

更新の自動化

更新ファイルを探したり、それを手動でダウンロードする必要はありません。F-Secure 自動更新エージェントを使用すると、F-Secure がパターン ファイルの更新を作成したときにそれを自動的にダウンロードします。

8.1.1 F-Secure 自動更新エージェントの使用

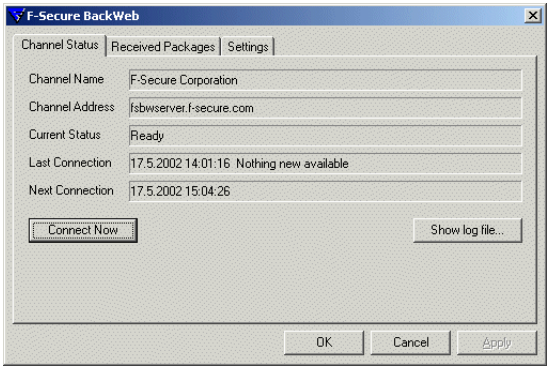
F-Secure 自動更新エージェントは透過的および自動的に動作します。F-Secure 自動更新エージェントのユーザ インタフェースは設定変更とアプリケーションの動作確認にのみ使用します。

F-Secure 自動更新エージェントのユーザ インタフェースは、アプリケーション リストから [F-Secure 自動更新エージェント] を選択し、[**プロパティ**] ボタンをクリックすると表示される、[F-Secure の設定と統計] ウィンドウから使用できます。[F-Secure の設定と統計] ウィンドウは、システム トレイの アイコンをダブルクリックしても表示できます。

F-Secure 管理エージェントがインストールされていない場合、[F-Secure の設定と統計] ウィンドウを開けないときは、システム トレイにある (F-Secure 自動更新エージェントのアイコン) をダブルクリックして開きます。F-Secure 管理エージェントがインストールされている場合、このアイコンは表示されません。

[F-Secure 自動更新エージェント] ウィンドウには、[通信路のステータス]、[受信パッケージ]、[設定] の 3 つのタブがあります。

通信路のステータス



[通信路のステータス] ページには、次の情報が表示されます。

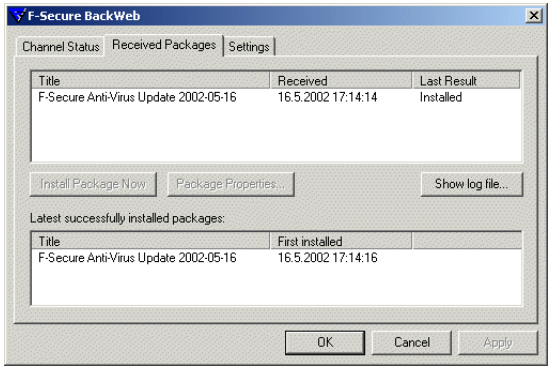
- 通信路名： ここには「F-Secure Corporation」と表示されます。
- 通信路のアドレス： サーバのインターネット アドレスです。
- 現在のステータス： 通信路の現在のステータス。たとえば、[接続中]、[ダウンロード中] などが表示されます。[待機中] は、クライアントが次のスケジュールされた接続を待機している状態にあることを示しています。
- 前回の接続： 通常は、「新しい情報はありません」と表示されます。これは、サーバへの接続は正常に確立されたが、ダウンロードする新しい情報がなかったことを表しています。「通信路が更新されました」は、接続が確立され、いくつかのファイルがダウンロードされたことを示しています。ダウンロードしたファイルは、パターン ファイルであるとはかぎらず、ニュース コンテンツや自動更新エージェントの内部ファイルであることもあります。前回ダウンロードした最新のアンチウィルスの更新ファイルは、[受信パッケージ] ページに表示されます。
- 次回の接続：

[**今すぐ接続**] ボタンをクリックすると、通信路を手動で起動し、新しいコンテンツを検索することができます。そうでない場合は、約 60 分間隔で実行されます。インターネットに接続されている必要があり、ダイヤルアップ接続は開始されないことに注意してください。

［ログ ファイルを表示］ボタンをクリックすると、F-Secure 自動更新エージェントの動作の詳細ログを表示します。通常、ログを表示する必要はありませんが、クライアントが正しく動作していないと思われる場合に問題を解決するのに役立ちます。

受信パッケージ

［受信パッケージ］ページには、前回受信した最新の F-Secure アンチウィルス パターン ファイルの情報が表示されます。ウィルス ニュースは表示されません。



パッケージのタイトルと、受信日時のほかに、［前回の結果］列が表示されます。パターン ファイル更新の結果には、次の状態が表示されます。

- **インストールされました**
  ファイルがダウンロード先ディレクトリに格納されたこと（および、既存のファイルが削除されたこと）を示します。通信ディレクトリを更新すると、このように表示されます。F-Secure 自動更新エージェントは、新しいファイルが F-Secure アンチウィルス ホストによって使用されているかどうかは表示できません。
- **インストールされていません**
  この場合は、いくつかのエラーが発生し、ファイルがダウンロード先ディレクトリに格納されなかったことを示しています。F-Secure 自動更新エージェントは、インストールが正常に完了するまで 1 分間隔で自動的に再試行を繰り返します。エラー

メッセージを表示するには、データベースの更新ファイルのタイトルを選択し、[**パッケージのプロパティ**] ボタンをクリックします。

[前回の結果] 列には、このパッケージの前回の結果が表示されます。つまり、ここにエラーが表示された場合でも、それ以前にパッケージが正常にインストールされていることがあります。ページの下部にある [前回インストールしたパッケージ] には、前回正常にインストールされたパターン ファイルのタイトルと、初めて正常にインストールされたときの日時が表示されます。

パッケージのインストールを手動で開始する場合は、パッケージをリストから選択して [**パッケージを今すぐインストールする**] をクリックします。

[**パッケージのプロパティ**] ボタンを使用すると、選択したパッケージに関するいくつかの追加情報が表示されます。インストールが失敗した場合、ここに前回のエラー メッセージが表示されます。

ログ ファイルは、[通信路のステータス] ページに加え、ここでも表示できます。

設定

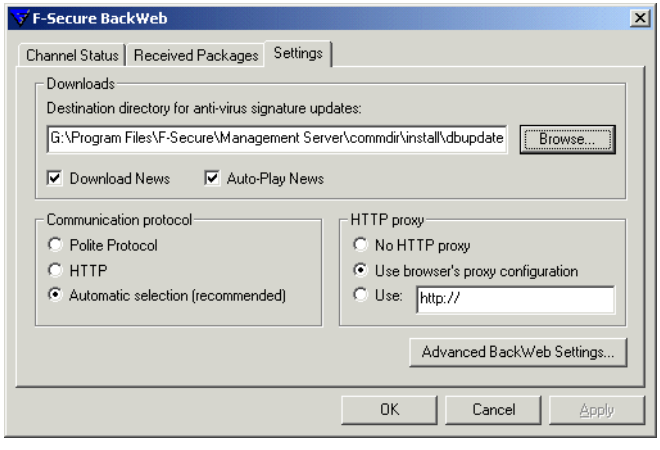


図 8-1 F-Secure 自動更新エージェントの［設定］ページ

［設定］ページでは、F-Secure 自動更新エージェントの最も重要な設定内容を表示したり変更することができます。［設定］ページには 3 つのセクションがあります。

- ［ダウンロード］- このセクションには更新されたパターンファイルのダウンロード先ディレクトリが表示されます。ダウンロード先ディレクトリを編集コントロールに直接入力するか、または［参照］ボタンを使ってディレクトリ参照ダイアログから選択することもできます。F-Secure 自動更新エージェントによる更新の対象がローカルにインストールされた F-Secure アンチウィルスだけの場合、ダウンロード先ディレクトリは自動的に検出され、編集コントロールと参照ボタンは使用できません。
- 通常、ダウンロード先ディレクトリは、F-Secure ポリシー マネージャ コンソールによって初期化され、F-Secure ポリシー マネージャ サーバで使用される通信ディレクトリですまた、場合によっては、ダウンロード先ディレクトリとして普通のサブディレクトリを指定できます。この場合、サブディレクトリの中身は空であるか、F-Secure パターン ファイルのみである必

要があります。また、さらにサブディレクトリを作成しないでください。ダウンロード先が空の場合、更新ファイルはダウンロードされますが、他の場所へはコピーされません。

- ［ニュースのダウンロード］および［ニュースの自動再生］チェックボックスは、コンピュータ ウィルス ニュースと F-Secure ニュースのダウンロードと自動再生をそれぞれ制御します。
- ［通信プロトコル］- デフォルトは、［自動選択］です。自動更新エージェントは、HTTP プロトコルを使用して F-Secure ポリシー マネージャに接続します。F-Secure 更新サーバに接続する場合は、ポライト プロトコルを使用します。
- [HTTP プロキシ］- このセクションでは、HTTP プロトコルで使用するプロキシ設定を定義できます。
- [HTTP プロキシを使用しない］- HTTP 通信にプロキシを使用しません。
- ［ブラウザのプロキシ設定を使用する］- 推奨されるデフォルト設定です。自動更新エージェントは Internet Explorer や Netscape ブラウザと同じ HTTP 設定を使用します。
- ［次のプロキシを使用する - http://］ー このオプションでは、プロキシ アドレスとポート番号をフィールドに入力して、使用する HTTP プロキシを手動で設定できます。
（例 : myproxy.mydomain.com:80）

これらの設定に対する変更は、［適用］または［OK］ボタンをクリックしたあとでのみ有効になります。これらのボタンをクリックする前であれば、［キャンセル］ボタンをクリックして変更をキャンセルできます。

また、通信および自動更新エージェントの高度な設定もできます。これらの設定を行うには、［**自動更新エージェントの詳細設定**］ボタンをクリックします。自動更新エージェントの［オプション］ダイアログが表示されます。ダイアログ上の［**ヘルプ**］ボタンをクリックすることで、指定可能な設定に関するすべての詳細情報を表示できます。

8.1.2 F-Secure 自動更新エージェントのトラブルシューティング

Q. どのようにすればパターン ファイルの更新が正常に機能していることを確認できますか？

A. F-Secure ポリシー マネージャから［F-Secure 自動更新エージェント］ウィンドウを開き、［受信パッケージ］タブを選択します。パターン ファイルがダウンロードされている場合は、［タイトル］の下に「F-Secure アンチウィルス 2003-07-31 更新」（日付は異なることがあります）のように表示されます。

［前回の結果］列を確認します。更新ファイルがダウンロード先ディレクトリに格納されている場合は、そのファイルの状態として「インストールされました」と表示されます。「インストールされていません」と表示されている場合は、更新ファイルのダウンロードは完了していますが、F-Secure 自動更新エージェントがそれをダウンロード先ディレクトリに配置できず、1 分間隔で配置を再試行することを示しています。ファイル名または［**パッケージのプロパティ**］ボタンをクリックすることで、エラー メッセージを表示できます。

［前回の結果］が「インストールされました」の場合は、［受信パッケージ］ページの［最初のインストール］列で日付と時間を確認してください。次に、Windows エクスプローラを開き、F-Secure アンチウィルスのフォルダ（通常は、C:¥Program Files¥F-Secure¥Anti-Virus）を選択します。［表示］メニューから［詳細］を選択し、ファイル リスト上部にある［更新日時］列のタイトルをクリックしてファイルを日付と時間で並べ替えます。［最初のインストール］列に表示されている日時とほぼ同じ日時のファイルがいくつか表示されます。通常はファイル名拡張子が .def、.avc、.set、または .dat であるファイルです。

ファイルはすぐには F-Secure アンチウィルス フォルダに格納されないことに注意してください。格納されるまでの時間は、F-Secure 管理エージェントのポーリング間隔によって異なります。デフォルトのポーリング間隔である 10 分の場合、更新ファイルは［最初のインストール］に表示されている時刻の 20 ～ 30 分以内にアンチウィルスのフォルダに格納されます。

Q. ［受信パッケージ］ページに、パターン ファイルの更新が「インストールされていません」と表示されます。どのように対処したらよいでしょうか ?

A. パッケージのタイトルをクリックしてから［**パッケージのプロパティ**］ボタンをクリックしてエラー メッセージを確認します。

アンチウィルス パターン ファイルの更新ファイルのディレクトリが見つかりません。ディレクトリが存在しない、通信ディレクトリが破損している、またはクライアントが標準モードで、ディレクトリがネットワーク ドライブにある可能性があります。[F-Secure 自動更新エージェント］ウィンドウで［設定］ページを開き、［**変更**］をクリックしてダウンロード先ディレクトリを変更します。

ディスクの空き領域が不足しています。ダウンロード先ディレクトリのドライブに空き領域がありません。更新版をダウンロードできるようにドライブの空き領域を増やしてください。

一時ディレクトリを作成できませんでした。クライアントが NT アプリケーション モードの場合は、ログインしているユーザがダウンロード先ディレクトリの適切なアクセス権を持っていることを確認してください。ダウンロード先が通信ディレクトリの場合は、そのサブディレクトリに対しても同じアクセス権を持っている必要があります。ダウンロード先がその他のサブディレクトリの場合は、その親ディレクトリに対しても同じアクセス権を持っている必要があります。

データベースの更新ファイルのディレクトリを変更できませんでした。この問題は、他のアプリケーションがダウンロード先ディレクトリ内のファイルを開いていて、それが原因で削除できない場合に発生します。特に共有ディレクトリまたは F-Secure ポリシー マネージャ サーバ通信ディレクトリの場合は、ホストが以前の更新ファイルを取得しているときにディレクトリを変更しようとすると、この問題が発生します。クライアントは 1 分間隔で再試行します。しばらくして結果が「インストールされました」に変わった場合はエラーではありません。このため、少し時間をおいてから、結果が「インストールされました」に変わるかどうか確認してください。結

果が「インストールされました」に変わらなかった場合は、ダウンロード先ディレクトリがあるコンピュータのすべてのアプリケーションを閉じるか、再起動してください。クライアントが NT アプリケーション モードの場合は、前の段落にある「一時ディレクトリを作成できませんでした」の説明も参照してください。

Q. パターン ファイルの更新のステータスは［受信パッケージ］ページで「インストール済み」になっていますが、アンチウィルスのディレクトリには新しいファイルが存在しません。その理由を教えてください。

A. 更新ファイルをダウンロードして、通信ディレクトリに配置した後、F-Secure アンチウィルスはそこからすぐにファイルを取り出しません。取り出すまでの時間は、F-Secure 管理エージェントのポーリング間隔によって異なります。デフォルトのポーリング間隔の 10 分の場合、取り出すまでの時間は 20 ～ 30 分になります。

一元集中管理されたアンチウィルス ホストの場合は、F-Secure ポリシー マネージャ サーバの［パターン ファイルの更新］で［自動ポーリング］を有効にしていることを確認してください。

一元集中管理されたホストの場合は、[F-Secure 自動更新エージェント］ウィンドウで［設定］ページを開き、更新ファイルのダウンロード先ディレクトリとして適切な通信ディレクトリを選択していることを確認してください。確かでない場合は、http://www.f-secure.com/download-purchase/updates.shtml から Latest.zip をダウンロードし、それを F-Secure ポリシー マネージャ コンソールにインポートしてください。この方法では正常に更新できても F-Secure 自動更新エージェントでは更新できず、しかも［受信パッケージ］ページの更新ファイルのステータスが「インストールされました」になっている場合は、間違ったディレクトリに更新ファイルを配置するように F-Secure 自動更新エージェントを設定している可能性があります。

スタンドアロンの F-Secure アンチウィルスの場合は、F-Secure 自動更新エージェントをスタンドアロン モードでインストールしたことを確認してください。[F-Secure 自動更新エージェント］ウィンドウで［設定］ページを開きます。［**変更**］ボタンが使用できなくなっていることを確認してください。

Q. F-Secure 自動更新エージェントをインストールしましたが、パターン ファイルがダウンロードされません。問題は ?

A. [F-Secure 自動更新エージェント] ウィンドウで [受信パッケージ] タブを選択し、パターン ファイルの更新パッケージが表示されていないことを確認します。

[F-Secure 自動更新エージェント] ウィンドウで [通信路のステータス] ページを選択します。[通信路名] と [通信路のアドレス] フィールドが空の場合は、クライアントが F-Secure 自動更新エージェント サーバにまだ接続していません。それ以外の場合は、インターネット接続に問題がないことを確認します (ダイヤルアップ接続を使用している場合は、通信を確立します)。[現在のステータス] が「待機中」になっている場合は、[**今すぐ接続**] をクリックして、すぐにクライアントをサーバに接続してください。初めてパターン ファイルをダウンロードするときに大量のインターネット トラフィックがあると、ダウンロードに時間がかかることがあります。

クライアントがサーバに接続できない場合は、まずブラウザがインターネットにアクセスできることを確認してください。確認するには、ブラウザを開いて、http://www.f-secure.com/ に接続します。正常に接続されたか確認してください。正常に接続されなかった場合は、ネットワーク管理者に連絡するか、ダイヤルアップ設定を確認してください。正しく接続されたら、[設定] ページを選択します。[通信] セクションで「ポライト エージェント」が選択されている場合は、HTTP に変更してください。プロトコルをポライト エージェントから HTTP (あるいはその逆) に変更した場合は、[OK] をクリックした後に自動更新エージェントを再起動することが求められます。プロトコルの変更は、クライアントを再起動するまで有効になりません。

プロトコルを HTTP に変更しても問題が解決しない場合は、ブラウザでインターネット オプションを開き、HTTP プロキシ サーバ経由で接続しているかどうか確認してください。確認方法の例をいくつか示します。

- Internet Explorer 4.0 の場合
  [表示] メニューで [インターネット オプション] を選択します。[接続] タブをクリックします。[プロキシ サーバ] セクションを参照します。[プロキシ サーバを使用してインター

ネットにアクセス] オプションがオンになっていて、アドレスとポートが定義されている場合は、HTTP プロキシ サーバを使用しています。[プロキシ サーバを使用してインターネットにアクセス] オプションがオフになっていて、[アドレス] セクションのプロキシ サーバの設定が淡色表示されている場合は、[詳細] タブをクリックしてアドレスを削除し、ポート 0 を指定します。

- Netscape Navigator 4.6 の場合
  [編集] メニューで [設定] を選択します。[詳細] カテゴリを開き、[プロキシ] オプションを選択します。[手動でプロキシを設定する] がオンになっている場合は、[**表示**] をクリックして指定した HTTP プロキシ サーバのアドレスとポート番号を取得します。

HTTP プロキシ サーバ経由で接続していることが確認できたら、[F-Secure 自動更新エージェント] ウィンドウの [設定] ページにある [HTTP プロキシを使用] チェックボックスをオンにして、ブラウザから取得したプロキシ サーバのアドレスとポート番号をそれぞれのフィールドに入力します（例： myproxy.mydomain.com:80）。

プロキシ サーバ経由で接続しない場合は、[HTTP プロキシを使用] オプションがオフになっていることを確認します。

これらの操作により、自動更新エージェントによる接続とコンテンツ受信が可能になります。クライアントは正しく設定されているのにコンテンツを受け取れない場合は、HTTP 要求を発信でき、それに対する応答を着信できるようにファイアウォールが設定されていることをネットワーク管理者に確認してもらってください。

- ダイヤルアップ接続を使用している場合は、[設定] ページで [自動更新エージェントの詳細設定] をクリックし、[接続] タブの [インターネット接続] オプションが [接続を検出] になっていることを確認してください。

Q. 自動更新エージェントのタスクバー アイコンをクリックすると表示されるメニューから［自動更新エージェントをシャットダウン］コマンドを選択しました。アイコンは一時的に消えましたが、しばらくすると再び Windows タスクバーに表示されました。なぜこのようになるのでしょうか ?

A. F-Secure 自動更新エージェントが、Windows NT に標準モードまたはスタンドアロン モードでインストールされています。このソフトウェアは Windows NT サービスとして実行されているため、シャットダウンしても自動的に再起動されます。自動更新エージェントのダウンロードを一時的に停止したい場合は、自動更新エージェントのタスクバー メニューから［ダウンロードを中止］を選択してください。自動更新エージェントを再度有効にするには、［ダウンロードを再開］を選択します。

Q. [F-Secure の設定と統計］ウィンドウで、F-Secure 自動更新エージェントのステータスが［無効］になっているのはなぜですか ?

A. F-Secure 自動更新エージェントが起動されていない場合に、このように表示されます。まだ起動していない、または終了してしまった、あるいは、自動更新エージェントのコア コンポーネントをアンインストールしたのに F-Secure のエクステンションがまだ残っていることが原因として考えられます。

Windows を起動した直後の場合は、自動更新アイコンが表示されてステータスが［有効］になるまで待ってください。Windows 98 を使用している場合、またはクライアントを NT アプリケーション モードでインストールした場合は、クライアントを自動更新エージェント Windows デスクトップまたは［スタート］メニューから起動してください。

問題が解決しない場合、または自動更新エージェントのアイコンがタスクバーに表示されているのに［F-Secure の設定と統計］ウィンドウでステータスが［有効］に変わらない場合は、インストールされている F-Secure 自動更新エージェントが破損している可能性があります。この場合は、クライアントをいったんアンインストールしてから再インストールしてください。

Q. [F-Secure の設定と統計] ウィンドウで、F-Secure 自動更新エージェントのステータスが [停止中] になっているのはなぜですか ?

A. 自動更新エージェント タスクバー メニューからダウンロードを中断したか、ディスクの空き領域不足などの問題が発生した可能性があります。タスクバー メニューから [ダウンロードを再開] を選択するか、接続で問題が発生していないことを確認してください。

8.2 F-Secure ポリシー マネージャ プロキシによる自動更新

F-Secure アンチウィルス プロキシ自動更新の情報と手順については、『F-Secure ポリシー マネージャ プロキシ管理者用ガイド』を参照してください。

9 LINUX 上での F-SECURE ポリシー マネージャ

概要 178
インストール 178
設定 182
アンインストール 182
FAQ（よくある質問） 185

9.1 概要

F-Secure ポリシー マネージャは、Linux にもインストールできます。

9.1.1 Windows 版と Linux 版の違い

Linux 上で動作する F-Secure ポリシー マネージャ コンソールでは、次のサービスを利用できません。:

- インストール情報の送信
- Windows インストール パッケージ (MSI) のエキスポート
- ネットワーク上のワークステーションの自動発見

9.1.2 対応ディストリビューション

F-Secure ポリシー マネージャは、Debian パッケージ管理 (DEB) システムおよび Redhat Package Management (RPM) システムに基づく、多数の Linux ディストリビューションに対応しています。これらの 2 つのシステムのコマンドは異なります。

対応ディストリビューション	パッケージ システム
Red Hat Enterprise Linux 4	RPM
Red Hat Enterprise Linux 3	RPM
SUSE Linux 10.0	RPM
SUSE Linux 9.x	RPM
SUSE Linux Enterprise Server 9	RPM
Debian GNU Linux Sarge 3.1	DEB

9.2 インストール

F-Secure ポリシー マネージャは、4 つのコンポーネントでインストールされます。これらは、次の順序でインストールする必要があります。

1. F-Secure 自動更新エージェント
2. F-Secure ポリシー マネージャ サーバ
3. F-Secure ポリシー マネージャ コンソール
4. F-Secure ポリシー マネージャ Web レポート

F-Secure ポリシー マネージャ サーバ､F-Secure ポリシー マネージャ Web レポート、および F-Secure 自動更新エージェントは、同じコンピュータにインストールする必要があります。Windows でも Linux でもかまいません。

F-Secure ポリシー マネージャ コンソールは、同じコンピュータまたは別のコンピュータにインストールできます。Windows でも Linux でもかまいません。

9.2.1 F-Secure 自動更新エージェントのインストール

1. root としてログインします。
2. ターミナルを開きます。
3. 次のコマンドを入力してインストールします。

Debian ベースのディストリビューション	RPM ベースのディストリビューション
dpkg -i f-secure-automatic-update-agent_<version_number>.<build number>_i386.deb	rpm -i f-secure-automatic-update-agent-<version_number>.<build number>-1.i386.rpm

F-Secure 自動更新エージェント が実行されました。以降、コンピュータの再起動時に自動的に起動されます。

9.2.2 F-Secure ポリシー マネージャ サーバのインストール

1. root としてログインします。
2. ターミナルを開きます。

3. 次のコマンドを入力してインストールします。

Debian ベースのディストリビューション	RPM ベースのディストリビューション
dpkg -i f-secure-policy-manager-server_<version_number>.<build number>_i386.deb	rpm -i f-secure-policy-manager-server-<version_number>.<build number>-1.i386.rpm

4. 次のコマンドを入力して設定します。

   /opt/f-secure/fspms/bin/fspms-config

   画面に表示される質問に答えます。

   それぞれの質問で ENTER キーを押すと、デフォルト設定（括弧の中に表示された設定）が選択されます。

F-Secure ポリシー マネージャ サーバが起動します。以降、コンピュータの再起動時に自動的に起動されるようになります。

9.2.3 F-Secure ポリシー マネージャ コンソールのインストール

1. root としてログインします。
2. ターミナルを開きます。
3. 次のコマンドを入力してインストールします。

Debian ベースのディストリビューション	RPM ベースのディストリビューション
dpkg -i f-secure-policy-manager-console_<version_number>.<build number>_i386.deb	rpm -i f-secure-policy-manager-console-<version_number>.<build number>-1.i386.rpm

新しい fspmc というユーザ グループが自動的に作成されます。
F-Secure ポリシー マネージャ コンソールを実行するユーザを、fspmc ユーザ グループに追加する必要があります。

4. ユーザが属しているグループを確認します。

   groups <ユーザ ID>

たとえば、ユーザが Yamada の場合は、次のように入力します。

groups Yamada

5. このユーザを fspmc グループに追加します。

   /usr/sbin/usermod -G fsmpc,<ユーザが現在所属しているグループ（カンマ区切りのリスト）><ユーザ ID>

   たとえば、Yamada が normal_users および administrators グループに属している場合、コマンドは次のようになります。

   /usr/sbin/usermod -G fsmpc,normal_users,administrators Tom

   カンマ区切りのグループ リストは、ユーザが以前に所属していたグループを置き換えます。

6. ログアウトします。
7. ログインします。
8. 次のコマンドを入力して起動します。

   /opt/f-secure/fspmc/fspmc

   このコマンドを最初に入力したときには、設定を完了するためにいくつかの質問が表示されます。これらの質問は Windows 版の場合と同じです（『インストールの手順』(P64) を参照してください）。

9.2.4 F-Secure ポリシー マネージャ Web レポートのインストール

1. root としてログインします。
2. ターミナルを開きます。
3. 次のコマンドを入力してインストールします。

Debian ベースのディストリビューション	RPM ベースのディストリビューション
dpkg -i f-secure-policy-manager-web-reporting_<version_number>.<buildnumber>_i386.deb	rpm -i f-secure-policy-manager-web-reporting-<version_number>.<buildnumber>-1.i386.rpm

4. 次のコマンドを入力して設定します。
   /opt/f-secure/fspmwr/bin/fspmwr-config
   画面に表示される質問に答えます。
   それぞれの質問で ENTER キーを押すと、デフォルト設定（括弧の中に表示された設定）が選択されます。
5. 次のコマンドを入力して起動します。
   /etc/init.d/fspmwr start

9.3 設定

F-Secure ポリシー マネージャ コンポーネントには、個別の設定スクリプトが用意されています。各コンポーネントを設定するには、対応する設定コマンドを入力し、質問に答えます。

F-Secure ポリシー マネージャのコンポーネント	設定コマンド
F-Secure ポリシー マネージャ サーバ	/opt/f-secure/fspms/bin/fspms-config
F-Secure ポリシー マネージャ Web レポート	/opt/f-secure/fspmwr/bin/fspmwr-config

9.4 アンインストール

4 つのコンポーネントを、次の順序でアンインストールする必要があります。

1. F-Secure ポリシー マネージャ Web レポート
2. F-Secure ポリシー マネージャ コンソール
3. F-Secure ポリシー マネージャ サーバ
4. F-Secure 自動更新エージェント

9.4.1 F-Secure ポリシー マネージャ Web レポートのアンインストール

1. root としてログインします。
2. ターミナルを開きます。
3. 次のコマンドを入力します。

Debian ベースのディストリビューション	RPM ベースのディストリビューション
dpkg -r f-secure-policy-manager-web-reporting	rpm -e f-secure-policy-manager-web-reporting

ログ ファイルと設定ファイルは削除されません。これらのファイルは重要な情報を含んでいることで、置き換えできません。これらのファイルを削除するには、次のコマンドを入力します。

```
rm -rf /opt/f-secure/fspmwr
```

9.4.2 F-Secure ポリシー マネージャ コンソールのアンインストール

1. root としてログインします。
1. ターミナルを開きます。
2. 次のコマンドを入力します。

Debian ベースのディストリビューション	RPM ベースのディストリビューション
dpkg -r f-secure-policy-manager-console	rpm -e f-secure-policy-manager-console

ログ ファイルと設定ファイルは削除されません。これらのファイルは重要な情報を含んでいることで、置き換えできません。これらのファイルを削除するには、次のコマンドを入力します。

```
rm -rf /opt/f-secure/fspmc
```

9.4.3 F-Secure ポリシー マネージャ サーバのアンインストール

1. root としてログインします。
2. ターミナルを開きます。
3. 次のコマンドを入力します。

Debian ベースのディストリビューション	RPM ベースのディストリビューション
dpkg -r f-secure-policy-manager-server	rpm -e f-secure-policy-manager-server

ログ ファイルと設定ファイルは削除されません。これらのファイルは有益な情報を含んでいることで、置き換えできません。これらのファイルを削除するには、次のコマンドを入力します。

```
rm -rf /var/opt/f-secure/fsaus
rm -rf /var/opt/f-secure/fspms
rm -rf /etc/opt/f-secure/fspms
rm -rf /etc/opt/f-secure/fsaus
```

9.4.4 F-Secure 自動更新エージェントのアンインストール

1. root としてログインします。
2. ターミナルを開きます。
3. 次のコマンドを入力します。

Debian ベースのディストリビューション	RPM ベースのディストリビューション
dpkg -r f-secure-automatic-update-agent	rpm -e f-secure-automatic-update-agent

9.5 FAQ（よくある質問）

Q. F-Secure ポリシー マネージャ コンソールが起動しません。

A. ランタイム エラーと警告は次のファイルに記録されます。このファイルを参照して、原因をまず確認します。

/opt/f-secure/fspmc/lib/Administrator.error.log

Q. F-Secure ポリシー マネージャ サーバが起動しません。

A. ランタイム エラー、警告、およびその他の情報は次のファイルに記録されます。このファイルを参照して、原因をまず確認します。

/opt/f-secure/fspms/logs/error_log

/opt/f-secure/fsaus/log/fsaus/log/log

/opt/f-secure/fsaus/log/fsaus/log/fsaus_watchdog_log

一般的な原因として、別のサーバがすでにポート 80 と 8080 を使用している可能性があります。これは、以下の手順で確認できます。

a. root としてログインします。

b. 次のコマンドを入力します。

```
netstat -t -p
```

または

```
fuser -vn tcp 80 8080
```

Q. パターン ファイルを手動で更新するにはどうすればよいでしょうか?

A. 次のコマンドを入力して、更新ツールを実行します。

```
sudo -u fspms /opt/f-secure/fspms/bin/fsavupd
```

Q. F-Secure ポリシー マネージャ サーバと F-Secure 自動更新エージェントが正常に動作しているにもかかわらず、F-Secure ポリシー マネージャ サーバが新しいパターン ファイルを配布しません。

A. 次のコマンドを入力すると、F-Secure ポリシー マネージャ サーバと F-Secure 自動更新エージェント間の通信エラーに関する情報を参照できます。

```
sudo -u fspms /opt/f-secure/fspms/bin/fsavupd —debug
```

Q. Linux 版の F-Secure ポリシー マネージャ コンソールのファイルはどこにありますか ?

A. すべてのファイルとその場所のリストを表示するには、次のコマンドを入力します。

Debian ベースのディストリビューション	RPM ベースのディストリビューション
dpkg -L f-secure-policy-manager-console	rpm -ql f-secure-policy-manager-console

Q. Linux 版の F-Secure ポリシー マネージャ サーバのログ ファイル、設定ファイル、および通信ディレクトリはどこにありますか ?

A. すべてのファイルとその場所のリストを表示するには、次のコマンドを入力します。

Debian ベースのディストリビューション	RPM ベースのディストリビューション
dpkg -L f-secure-policy-manager-server	rpm -ql f-secure-policy-manager-server

以下のファイルは次の場所にあります。

項目	ファイルシステム内の場所
ログ ファイル	/var/opt/f-secure/fspms/logs
設定ファイル	/etc/opt/f-secure/fspms/
通信ディレクトリ	/var/opt/f-secure/fspms/commdir

Q. F-Secure ポリシー マネージャ サーバが要求を受信するポートを変更するにはどうすればよいでしょうか？

A. 『httpd.conf ファイルを編集して、F-Secure ポリシー マネージャ サーバへのアクセスを別に定義した IP アドレスのみに制限します。』(P30) を参照してください。

Q. 設定ファイルを変更した後、F-Secure ポリシー マネージャ サーバを再起動するにはどうすればよいでしょうか？

A. F-Secure ポリシー マネージャ サーバを再起動するには、以下の手順を実行します。

a. root としてログインします。
b. 次のコマンドを入力します。
   /etc/init.d/fspms restart

Q. F-Secure ポリシー マネージャ サーバの動作状態に関する情報をどこかで確認できますか？

A. 次のコマンドを入力します。

/etc/init.d/fspms status

Q. パターン ファイルの自動更新スケジュールはどうすれば設定できますか？

A. F-Secure ポリシー マネージャ サーバ設定スクリプトを実行します。

/opt/f-secure/fspms/bin/fspms-config

Q. F-Secure 自動更新エージェントが F-Secure Policy Manager Proxy を使用するように設定するにはどうすればよいでしょうか？

A. F-Secure Policy Manager Proxy を使用するには、以下の手順を実行します。

a. /opt/f-secure/fsaua/etc/fsaua_config ファイルをテキスト エディタで開きます。
b. 次のように、ファイルに update_proxies=host:port の行を追加します。

update_proxies=proxy.domain.com:80

複数のプロキシを設定する場合はカンマ区切りで記述します。
update_proxies=proxy.domain.com:80,back_up_proxy.domain2.com:80

c. F-Secure 自動更新エージェントを再起動して、変更を有効にします。

/etc/init.d/fsaua restart

Q. F-Secure 自動更新エージェントで HTTP プロキシを使用するにはどうすればよいでしょうか ?

A. HTTP プロキシは、/opt/f-secure/fsaua/etc/fsaua_config ファイルで設定します。

a. /opt/f-secure/fsaua/etc/fsaua_config ファイルをテキスト エディタで開きます。

b. 次のように、ファイルに http_proxies=user:password@host:port の行を追加します。

http_proxies=Tom:toms_password@proxy.domain.com:80

複数のプロキシを設定する場合はカンマ区切りで記述します。

http_proxies=Tom:toms_password@proxy.domain.com:80,Ann:anns_password@back_upproxy.domain2.com:80

c. F-Secure 自動更新エージェントを再起動して、変更を有効にします。

/etc/init.d/fsaua restart

Q. 設定ファイルを変更した後、F-Secure 自動更新エージェントを再起動するにはどうすればよいでしょうか ?

A. F-Secure 自動更新エージェントを再起動するには、次のコマンドを入力します。

/etc/init.d/fsaua restart

10 Web レポート

概要 190
はじめに 190
Web レポート クライアントのシステム要件 191
レポートの生成および表示 191
Web レポートの管理 197
Web レポートのエラー メッセージおよびトラブル シューティング 202

10.1 概要

この章では、以下の項目について説明します。

- F-Secure ポリシー マネージャ Web レポートと、その機能の紹介
- Web レポートを生成および表示する方法
- F-Secure ポリシー マネージャ Web レポート アプリケーションを設定および管理する方法。Web レポートへのアクセスを制限または許可する方法や、Web レポート データベースをバックアップおよび復元する方法など。

Web レポートは、F-Secure ポリシー マネージャ サーバのセットアップの一部としてインストールされます。詳細については、『インストールの手順』(P33) を参照してください。

F-Secure ポリシー マネージャ Web レポートを高度なセキュリティ環境にインストールする際の注意事項については、『F-Secure ポリシー マネージャ Web レポートを高度なセキュリティ環境にインストールする』(P31) を参照してください。

10.2 はじめに

F-Secure ポリシー マネージャ Web レポートは、F-Secure ポリシー マネージャ サーバに付属する、視覚的なレポート システムです。F-Secure ポリシー マネージャ Web レポートのグラフ形式の詳細レポートを使用すると、ウィルス発生に対して保護されていないコンピュータや被害を受けやすいコンピュータを識別することができます。F-Secure ポリシー マネージャ Web レポートでは、Web ベースのインタフェースを使用して、過去のデータに基づいてグラフ形式のレポートをすばやく作成することができます。F-Secure 管理エージェントから F-Secure ポリシー マネージャ サーバに送信された F-Secure クライアント セキュリティの警告やステータス情報を利用して、多様で便利なレポートとクエリを作成できます。レポートを HTML 形式でエキスポートすることができます。

F-Secure ポリシー マネージャ Web レポートは、強力な SQL データベースと統合されており、あらゆる規模の企業に適しています。Web レポートのデータベースは、現在 F-Secure ポリシー マネージャ サーバに格納されているすべてのデータを収集し、到着した新規データを追加します。収集されるデータには、警告のデータの大半、およびインクレメンタル ポリシー ファイル（.ipf）のデータの一部が含まれます。Web レポートのデータベースにデータを格納する期間を設定したり、データベースのパフォーマンスを最適化することができます。

10.3 Web レポート クライアントのシステム要件

F-Secure ポリシー マネージャ Web レポートによって生成されたレポートを表示するには、コンピュータに Internet Explorer 6 SP1、Netscape Communicator 7.1、Mozilla Firefox 1.x などの最近のインターネット ブラウザがインストールされている必要があります。

10.4 レポートの生成および表示

生成できる一般的なレポートのタイプには、現在のセキュリティ状況を示す棒グラフや円グラフ、トレンド レポート、詳細なリスト レポートなどがあります。正確なレポートおよび使用できるレポート テンプレートを表示するには、Web レポートのユーザ インタフェースでいずれかのページを選択します（[ウィルス保護の概要]、[インターネット防御の概要]、[警告]、[インストールされているソフトウェア]、および [ホストのプロパティ]）。

大規模な環境では、F-Secure ポリシー マネージャ Web レポートの起動に時間がかかる場合があります。Web レポートの起動時に、使用できないレポートにアクセスしようとすると、エラー メッセージが表示されます。詳細については、『Web レポートのエラー メッセージおよびトラブルシューティング』（P202）を参照してください。

10.4.1 Web レポートの表示に必要なブラウザの設定

Web レポートの使用を開始する場合は、ご使用のブラウザの設定を調べて、常に最新のレポートをロードし、キャッシュに格納されたレポートの一部または全体は表示しないように設定されていることを確認することをお勧めします。レポート情報の一部がキャッシュから取得された場合は、ブラウザにエラー メッセージが表示される場合があります。

Netscape Communicator および Mozilla のブラウザのキャッシュについては、次の設定をお勧めします。

[キャッシュにあるページとネットワーク上のページの比較]

- [ページにアクセスするたび]
  Netscape で Web ページを表示するたびに、キャッシュ内のページと比較するには、このオプションを選択します。
- [ページが時間切れの場合]
  サーバによりページの期限が切れていると判断された場合に、Netscape でその Web ページをキャッシュ内のページと比較するには、このオプションを選択します。

Microsoft Internet Explorer のブラウザのキャッシュについては、次の設定をお勧めします。

[保存しているページの新しいバージョンの確認]

- [ページを表示するごとに確認する]
  Internet Explorer で Web ページを表示するたびに、キャッシュ内のページと比較するには、このオプションを選択します。
- [自動的に確認する]
  Internet Explorer でページの新しいバージョンを自動的に確認するには、このオプションを選択します。

Cookie

ご使用のブラウザで Cookie を有効にすることもお勧めします。こうすると、簡単にポリシー ドメイン ツリーを参照できるようになります。保存されているレポートにアクセスできればよいという場合は、Cookie を有効にする必要はありません。

10.4.2 レポートの生成

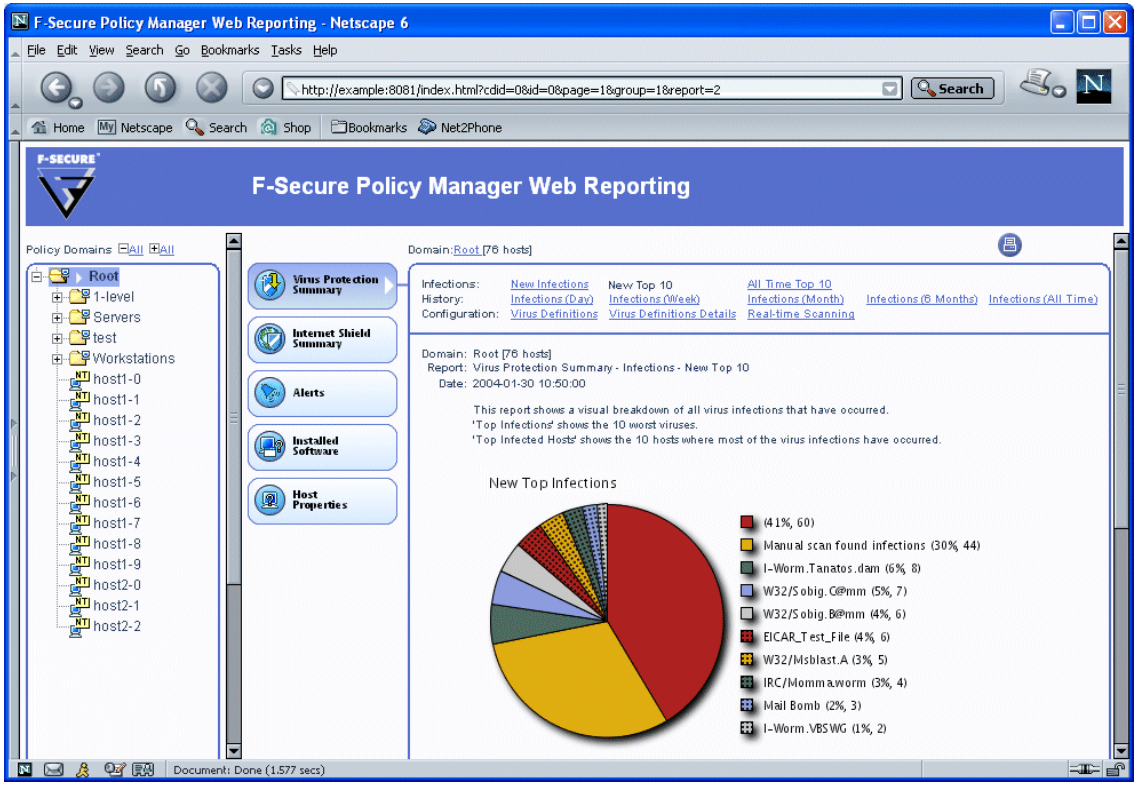
次の方法で、Web レポートを生成できます。

1. まず、F-Secure ポリシー マネージャ Web レポートのメイン ページを開きます。ブラウザに、F-Secure ポリシー マネージャ サーバの名前または IP アドレスを入力し、続けて Web レポートのポートを（コロンで区切って）入力します。たとえば、「fspms.example.com:8081」と入力します。

   Web レポートにローカルでアクセスする場合は、次のように、[スタート] メニューから Web レポートにアクセスすることもできます。[スタート] > [F-Secure ポリシー マネージャ サーバ] > [Web レポート] の順に選択します。

2. Web レポートのページが開くまで待ちます。大規模な環境の場合は、表示されるまでに時間がかかる場合があります。

   F-Secure ポリシー マネージャ Web レポートのページが開くと、現在選択されているレポート分類のデフォルトのレポートが表示されます。[ポリシー ドメイン] ウィンドウでは、デフォルトで [ルート] が選択されています。



3. 新規レポートを表示するには、まずレポートを生成するドメイン、サブドメイン、またはホストを選択します。
4. 次に、レポートの分類（[ウィルス保護の概要]、[インターネット防御の概要]、[警告]、[インストールされているソフトウェア]、および [ホストのプロパティ]）と、生成する正確なレポートを選択します。
5. メイン ウィンドウの下部にレポートが表示されるまで待ちます。

10.4.3 印刷可能なレポートの作成

印刷可能なページを表示するには、ページの右上隅にある アイコンをクリックします。新しいブラウザ ウィンドウが開き、メイン フレームのコンテンツが印刷可能な形式で表示され、ブラウザの印刷機能を使用してページを印刷することができます。

また、ご使用のブラウザの［名前を付けて保存］または［ページに名前を付けて保存］オプションを使用すると、レポートを保存して後で使用することができます。保存オプションでは、次のようにして完全な Web ページ（画像を含む）を保存します。

- Microsoft Internet Explorer 6 を使用している場合は、まず［ファイル］メニューの［名前を付けて保存］を選択します。［Web ページの保存］ウィンドウが表示されたら、［ファイルの種類］ドロップダウン メニューの［Web ページ、完全］を選択します。
- Netscape 7.1 または Mozilla 1.4 を使用している場合は、［ファイル］メニューの［ページに名前を付けて保存］を選択します。

10.4.4 自動化されたレポートの生成に使用する固有の URL の生成

固有の URL を生成して、自動化されたレポートの生成に使用することもできます。固有の URL アドレスには別に監視するレポートの分類、レポートのタイプ、ポリシー ドメインが含まれているため、次回同じレポートを生成する際にこれらの情報を選択する必要がありません。

次の 2 つの操作が可能です。

- 監視対象を含むレポートを生成し、そのレポートへのリンクをコンピュータ（デスクトップ、ブックマーク、またはその他の場所）に追加します。このリンクを使用して、次に F-Secure ポリシー マネージャ Web レポートにアクセスしたときに、レポートが再生成されて最新のデータが表示されます。
- 生成したレポートを保存しておいて、今後生成するレポートと現在の状況を比較することもできます。まず、印刷可能なページを生成し、ブラウザでページ全体を保存します。こうすると、いつでも「古い」レポートを参照できます。手順については、『印刷可能なレポートの作成』(P195) を参照してください。

10.5 Web レポートの管理

ここでは、最も一般的な F-Secure ポリシー マネージャ Web レポートの管理タスクについて説明します。

10.5.1 Web レポートの無効化

F-Secure ポリシー マネージャ Web レポートを無効にするには、コントロール パネルで［管理ツール］の［サービス］を使用して次の操作を行います。

1. Windows の［スタート］メニューで、コントロール パネルから［管理ツール］の［サービス］を開きます。
2. サービスのリストから［F-Secure ポリシー マネージャ Web レポート］を選択します。
3. ［アクション］メニューを開き、［プロパティ］を選択します。サービスを停止するには［停止］をクリックします。
4. スタートアップの種類を［手動］に設定します。Web レポートを一時的に停止する場合は、この手順をスキップします。
5. ［OK］をクリックします。

F-Secure ポリシー マネージャのセットアップを再実行して、Web レポートを無効にすることもできます。

10.5.2 Web レポートの有効化

前回インストール中に Web レポートを有効にしてから上記の手順を使用して無効にした場合にのみ、次の手順を使用して Web レポートを有効にすることができます。
セットアップを再実行すると、いつでも Web レポートを有効にすることができます。

F-Secure ポリシー マネージャ Web レポートを有効にするには、コントロール パネルで［管理ツール］の［サービス］を使用して次の操作を行います。

1. Windows の［スタート］メニューから［管理ツール］の［サービス］を開きます。
2. サービスのリストから［F-Secure ポリシー マネージャ Web レポート］を選択します。
3. ［アクション］メニューを開き、［プロパティ］を選択します。サービスを開始するには［**開始**］をクリックします。
4. スタートアップの種類を［自動］に設定します。
5. ［OK］をクリックします。

Web レポートを動作させるには、ポリシー マネージャ管理モジュールも有効にする必要があります。

10.5.3 Web レポートへの幅広いアクセスの制限または許可

F-Secure ポリシー マネージャ サーバのインストール先ディレクトリにある conf¥ ディレクトリに、httpd.conf という名前のファイルがあります。このファイルには、F-Secure ポリシー マネージャ サーバと F-Secure ポリシー マネージャ Web レポートの設定情報が記述されています。

設定を変更した場合、変更を有効にするには、F-Secure ポリシー マネージャ サーバを停止して再起動する必要があります。

Web レポートへのアクセス権には、ローカル マシンからのみのアクセス、すべての場所からのアクセス、IP アドレスで定義されたいくつかのホストからのアクセスの 3 種類を定義できます。

どのコンピュータからのアクセスも許可する（デフォルト）

デフォルトでは、ポリシー マネージャ サーバの Web レポート ポートにアクセスできるコンピュータであれば、どのコンピュータからでも F-Secure ポリシー マネージャ Web レポートにアクセスできます。これは、httpd.conf ファイル内の次のパラメータで定義されます。

```
Listen 8081
```

ローカル マシンからのアクセスだけを許可する

F-Secure ポリシー マネージャ Web レポートへのアクセスを、ローカル マシンからのみに許可することもできます。httpd.conf ファイルで、Web レポートのポートのパラメータを次のように設定します。

```
Listen 127.0.0.1:8081
```

Web レポートにアクセスできるホストのリストを指定する

F-Secure ポリシー マネージャ Web レポートへのアクセスを、個別に定義された特定の IP アドレスのみに許可することもできます。次に、httpd.conf ファイル セクションの編集例を示します。

```
#Web Reporting listen
Listen 8081


# Web Reporting port:
<VirtualHost _default_:8081>
  JkMount /* ajp13
  ErrorDocument 500 "ポリシー マネージャ サーバはポリシー マネージャ Web レポートにアクセスできませんでした。"
  <Location / >
    Order Deny,Allow
    Deny from all
    Allow from ip-address-1
    Allow from ip-address-2
    Allow from ip-address-3
  </Location>
</VirtualHost>
```

このようにすると、定義された IP アドレスのマシンにアクセスできるユーザだけが Web レポートを使用できます。

10.5.4 Web レポートのポートの変更

F-Secure ポリシー マネージャ Web レポートのポートを変更するには、F-Secure ポリシー マネージャ セットアップを再実行してから Web レポートのポートを変更する方法をお勧めします。詳細については、『インストールの手順』(P33) を参照してください。

Web レポートのポートは、httpd.conf ファイルを編集して変更することもできます。

1. F-Secure ポリシー マネージャ サーバを停止します。
2. httpd.conf ファイルで Web レポートのポート (Listen) および VirtualHost パラメータを編集して、新しいポート番号を含めます。
3. F-Secure ポリシー マネージャ サーバを起動します。

ポートが競合していると、F-Secure ポリシー マネージャ サーバは起動されず、ログ ファイルにエラー メッセージが出力されます。この場合は、別の未使用のポートを使用する必要があります。

10.5.5 Web レポート データベースのバックアップ コピーの作成

Web レポート データベースのバックアップをバックアップ メディアに作成するには、次の手順を実行します。

1. F-Secure ポリシー マネージャ Web レポート サービスを停止します。
2. 次のファイルを

   C:¥Program Files¥F-Secure¥Management Server 5¥Web Reporting¥firebird¥data¥fspmwr.fdb

   バックアップ メディアにコピーします。圧縮ユーティリティを使用して、ファイルを圧縮することもできます。圧縮ユーティリティを使用すると、バックアップしたデータベースがそのままの状態で残っているか確認することができます。

3. F-Secure ポリシー マネージャ Web レポート サービスを再起動します。

バックアップ コピーにより、履歴データの破損を防ぐことができます。また、Web レポート データベースの最大保存期間が変更されたときに削除される古いデータをアーカイブする場合にも使用できます（『Web レポート データベースの最大保存期間の変更』(P201) を参照）。

10.5.6 バックアップ コピーからの Web レポート データベースの復元

F-Secure ポリシー マネージャ Web レポート データベースをバックアップ コピーから復元するには、以下の手順を実行します。

1. F-Secure ポリシー マネージャ Web レポート サービスを停止します。
2. バックアップ メディアから次のディレクトリに fspmwr.fdb ファイルをコピーし、解凍します。
3. C:¥Program Files¥F-Secure¥Management Server 5¥Web Reporting¥firebird¥data
4. F-Secure ポリシー マネージャ Web レポート サービスを再起動します。

10.5.7 Web レポート データベースの最大保存期間の変更

トレンド データをデータベースに保存してから削除するまでの期間を設定することができます。デフォルトの期間は 1 年です。さらに長期間のトレンド レポートを生成するには、この期間をより長く設定します。トレンド データをもっと短い期間だけ保存するには、この期間をより短く設定します。

1. F-Secure ポリシー マネージャ Web レポート サービスを停止します。
2. Web レポートのディレクトリにある fspmwr.conf ファイルで、定義されている最大期間を変更します。使用する時間の単位は秒です。次に、設定ファイルの編集例を示します。

   ```
   #
   # The database data retaining time.The database data older than the current time
   # minus retaining time will be removed from the database permanently.
   #
   # Value:Use a retaining time measured in seconds.
   # Default:An empty value will set the default retaining time in use.The default
   #          retaining time is 12 months.
   #
   fspmwr.db.retain.time=31536000
   ```

3. F-Secure ポリシー マネージャ Web レポート サービスを再起動します。

   新しい設定は、すぐに使用されます。たとえば、データベースにデータが保存される最大期間を短くした場合は、新しい時間制限より古いデータはすべて削除されます。

10.6 Web レポートのエラー メッセージおよびトラブルシューティング

ここでは、F-Secure ポリシー マネージャ Web レポートのエラー メッセージと、Web レポート データベースのトラブルシューティングについて説明します。

10.6.1 エラー メッセージ

ブラウザのエラー メッセージ：「<location> にアクセスしようとして接続が拒否されました」

ブラウザは、Web レポートにまったくアクセスできませんでした。リンク先のマシンまたはポートが間違っているか、Web レポートがそのマシンにインストールされていないか、F-Secure ポリシー マネージャ サーバ サービスが実行されていない可能性があります。これらを順に確認してください。ファイアウォールによって接続が妨げられている可能性もあります。

エラー メッセージ：「F-Secure ポリシー マネージャ サーバは F-Secure ポリシー マネージャ Web レポートにアクセスできませんでした」

「ポリシー マネージャ サーバはポリシー マネージャ Web レポートにアクセスできませんでした」などのエラー メッセージが表示される場合は、F-Secure ポリシー マネージャ Web レポートが起動中です。しばらく待って、すべてのサービスがまだ起動されていないことが問題の原因であったことを確認してから、ページを再ロードしてください。

［管理ツール］の［サービス］を使用して Web レポートを手動で無効にした場合にも、エラー メッセージが表示されます。

サービスが起動されるまでにかかる時間は、管理対象の環境の規模によって異なります。CommDir から一部の警告を削除すると、起動時間を短くすることができます。

エラー メッセージ：「Web レポートは、<location> の F-Secure ポリシー マネージャ サーバとの接続を失いました。レポートのデータが失効済みなので、表示できません。」

F-Secure ポリシー マネージャ サーバが Web レポートにアクセスできない場合は、F-Secure ポリシー マネージャ サーバが長期に渡って過負荷になっていて、現在のデータが不正確であることを示している可能性があります。そのため、レポートが表示されません。このような場合は、ハードウェアをアップグレードする必要があります。

Web レポートに固有のエラーが発生した場合は、F-Secure ポリシー マネージャ サーバと Web レポート サービスの両方を再起動すると解決します。

エラー メッセージ：「Web レポートはデータベースとの接続を失いました。Web レポート サービスを再起動する必要があります。」

Web レポートからデータベースにアクセスできない場合は、Web レポート サービスを再起動する必要があります。それでも解決されない場合は、Web レポートを再インストールして、既存のデータベースを保持します。

10.6.2 トラブルシューティング

通常、F-Secure ポリシー マネージャ Web レポートが動作しない場合は、次の順序で試してください。

- ページを再ロードします。
- まだ起動されていないすべての処理で問題が起きる場合は、しばらく待ってからページを再ロードしてください。また、CommDir から不要な警告を削除すると、起動時間を短くすることができます。
- F-Secure ポリシー マネージャ Web レポート サービスを再起動します。
- F-Secure ポリシー マネージャ サーバを再起動します。
- コンピュータを再起動します。
- 既存の設定を残したまま、F-Secure ポリシー マネージャ サーバを再インストールします。
- それでも解決されない場合は、F-Secure ポリシー マネージャ Web レポート データベースをリセットするか、バックアップ コピーから復元します。

Web レポート データベースのリセット

通常、Web レポート サーバでは、現在設定されているデータの最大保存期間に基づいて、古いデータはデータベースから自動的に消去されます。ただし、データベースが本当に破損している場合は、破損したデータベース ファイルの上に空のデータベース ファイルをコピーすることもできます。設定するには、以下の手順を実行します。

1. F-Secure ポリシー マネージャ Web レポート サービスを停止します。
2. fspmwr.fdb に fspmwr.fdb.empty をコピーして、fspmwr.fdb を置換します。これらは同じディレクトリにあります。
   fspmwr.fdb.empty ファイルを誤って削除してしまった場合は、F-Secure ポリシー マネージャ サーバを再インストールする必要があります。
3. F-Secure ポリシー マネージャ Web レポート サービスを開始します。

11 F-SECURE ポリシー マネージャ プロキシ

概要 206
アンチウィルス プロキシとポリシー マネージャ プロキシの違い 206

11.1 概要

F-Secure ポリシー マネージャ プロキシは新しい製品で、F-Secure アンチウィルス プロキシとは異なります。F-Secure ポリシー マネージャ プロキシの詳細については、『F-Secure ポリシー マネージャ プロキシ管理者用ガイド』を参照してください。

F-Secure ポリシー マネージャ プロキシは、低速なネットワーク接続での負荷を大幅に減少させることにより、F-Secure クライアント セキュリティの分散インストールにおける帯域幅の問題を解決することができます。F-Secure ポリシー マネージャ サーバまたは F-Secure 更新サーバからパターン ファイルの更新を受信します。

F-Secure ポリシー マネージャ プロキシは、データベースの配布ポイントとして使用する対象ホストと同じリモート ネットワークに存在します。低速なネットワークには、F-Secure ポリシー マネージャ プロキシをそれぞれ 1 つ導入すると効率的です。F-Secure ポリシー マネージャ プロキシは F-Secure の配布サーバから直接パターン ファイルの更新を取得し、それらの更新は、F-Secure アンチウィルスが実行されているホストが F-Secure ポリシー マネージャ プロキシからローカルで取り出します。リモート オフィスのワークステーションはメイン オフィスのポリシー マネージャ サーバとも通信しますが、この通信は、リモートでのポリシー管理、ステータスの監視、および警告に制限されます。大量のデータベース更新トラフィックは同じローカル ネットワーク内の F-Secure アンチウィルス プロキシにリダイレクトされるため、マネージャのワークステーションと F-Secure ポリシー マネージャ サーバ間のネットワーク接続の負荷は大幅に軽減されます。

11.2 アンチウィルス プロキシとポリシー マネージャ プロキシの違い

F-Secure アンチウィルス プロキシは F-Secure クライアント セキュリティ 5.x で使用するように設計され、F-Secure ポリシー マネージャ プロキシは F-Secure クライアント セキュリティ 6.x で使用するように設計されています。

両プロキシは同じネットワークで共存できますが、対象していない製品の更新は提供できません。たとえば、F-Secure アンチウィルス プロキシは F-Secure クライアント セキュリティ 6.x 以降のバージョンに更新を配信することはできません。

F-Secure アンチウィルス プロキシはネットワーク内でスタンドアロンのサーバとして機能し、アップストリーム サーバの接続がない場合でも、ホストへ更新を提供できます。接続可能のアップストリーム サーバは F-Secure 更新サーバのみです。

F-Secure ポリシー マネージャ プロキシはネットワーク内で通常のプロキシとして機能し、更新をホストへ配信するためには、アップストリーム サーバが必要となります。F-Secure ポリシー マネージャ プロキシは F-Secure 更新サーバおよび F-Secure ポリシー マネージャ サーバの両サーバに接続できます。

12 トラブルシューティング

概要 210
FAQ（よくある質問）..... 210

12.1 概要

この章では、F-Secure ポリシー マネージャ サーバ と F-Secure ポリシー マネージャ コンソールのトラブルシューティング情報および FAQ（よくある質問）が記載されています。

F-Secure ポリシー マネージャ サーバの設定およびサーバが要求を受信するポートの変更方法については、『F-Secure ポリシー マネージャ サーバの設定』(P48) を参照してください。

12.2 FAQ（よくある質問）

Q. F-Secure ポリシー マネージャ サーバが起動しません。

A. 次のファイルに、ランタイム エラー、警告、およびその他の情報が含まれています。

<F-Secure>¥Management Server 5¥logs¥error.log

イベント ビューワ （Windows NT/2000/2003 では管理ツール）のアプリケーション ログが Apache サービスから「'ServerRoot must be a valid directory' or 'Syntax error on line 6」と表示した場合、以下を実行してください。

まず、httpd.conf に定義されている ServerRoot 行（デフォルトでは行 6）を確認します。問題がない場合、通信ディレクトリのアクセス権（プロパティ / 保護 / パーミッション）に fsms_<COMPUTERNAME> のユーザ アカウントが含まれていることを確認します。fsms_<COMPUTERNAME> が認証済みのユーザとして含まれていない場合、ユーザを手動で追加し、アクセス権を［フル コント

ロール] に設定します。管理サーバ 5 のディレクトリ（デフォルトでは C:¥Program Files¥F-Secure¥Management Server 5）とサブディレクトリにアクセス権を同様に設定します。変更後、F-Secure ポリシー マネージャ サーバのサービスを再開します。または、コンピュータを再起動します。

F-Secure ポリシー マネージャ サーバのインストール中に、fsms_<COMPUTERNAME> アカウントが作成され、このユーザ アカウントでサービスが起動します。通常のインストールでは、管理サーバ 5 のディレクトリ アクセス権限が自動的に設定されます。ディレクトリがコピーされたもの、またはバックアップから復元された場合、アクセス権限が正しく設定されていない可能性があります。このような場合、上記の手順を実行してアクセス権を正しく設定します。

Q. F-Secure ポリシー マネージャ サーバのログ ファイル、設定ファイル、および通信ディレクトリはどこにありますか？

A. ログ ファイルは次の場所にあります。

<F-Secure>¥Management Server 5¥logs

設定ファイルは次の場所にあります。

<F-Secure>¥Management Server 5¥conf

F-Secure ポリシー マネージャ サーバの通信ディレクトリは次の場所にあります。

<F-Secure>¥¥Management Server 5¥commdir

Q. F-Secure ポリシー マネージャ Web レポートのログ ファイルと設定ファイルはどこにありますか？

A. ログ ファイルは次の場所にあります。

<F-Secure>¥Management Server 5¥Web Reporting¥logs

設定ファイルは次の場所にあります。

<F-Secure>¥Management Server 5¥Web Reporting¥fspmwr.conf

<F-Secure>¥Management Server 5¥Web Reporting¥jetty¥etc¥fspmwr.xml

<F-Secure>¥Management Server 5¥Web Reporting¥firebird¥aliases.conf

<F-Secure>¥Management Server 5¥Web Reporting¥firebird¥firebird.conf

F-Secure ポリシー マネージャ サーバの設定ファイルもご覧ください。

<F-Secure>¥Management Server 5¥conf¥httpd.conf

<F-Secure>¥Management Server 5¥conf¥workers.properties

Q. F-Secure ポリシー マネージャ コンソールのログ ファイルはどこにありますか？

A. ログ ファイルは次の場所にあります。

<F-Secure>¥Administrator¥lib¥administrator.error.log

Q. サーバの機能を変更したら、F-Secure ポリシー マネージャ サーバは停止するのですか？

A. ドメインコントローラのサーバとメンバー / スタンドアロンのサーバは異なるアカウントを使用します。ドメイン コントローラではドメイン アカウントを、メンバー サーバではローカルのアカウントが使用されます。F-Secure ポリシー マネージャ サーバは固有のアカウントを使用するため、サーバの機能を変更した際にはこのアカウントは無効になります。

サーバの機能を変更した場合、F-Secure ポリシー マネージャ サーバを最も簡単に復元するには、F-Secure ポリシー マネージャ サーバを［既存の設定を保存する］を選択した状態で再インストールします。これによって、F-Secure ポリシー マネージャ サーバのアカウントは再作成され、ファイルのアクセス権限もすべて正しい設定にリセットされます。

Commdir を手動で新しい場所に移動した場合、移動先のディレクトリ ツリーに新しいアカウントのアクセス権を再設定する必要がある場合があります。

Q. F-Secure ポリシー マネージャ サーバはなぜシステムのアカウントではなく、固有のアカウントを使用するのでしょうか？

A. ポリシー マネージャ サーバのアカウント（fsms_<COMPUTERNAME>）はセキュリティの理由で使用されます。固有のアカウントを使用することによって、F-Secure ポリシー マネージャ サーバにセキュリティの脆弱性が発生した場合、問題は製品のみに影響し、全体のシステムに影響は及びません。システム アカウントが代わりに使用された場合、F-Secure ポリシー マネージャ サーバに万一のセキュリティ問題が発生した際に、システム全体に異常が発生する可能性があります。

Q. Windows のセキュリティを強化すると、F-Secure ポリシー マネージャ サーバの動作はどのように影響されますか？

A. アクセス権の制限、特に %SystemRoot% ディレクトリ（c:¥windows または c:¥winnt）に指定される制限は F-Secure ポリシー マネージャ サーバの起動を停止する可能性があります。ポリシー マネージャ固有のアカウント（fsms_<COMPUTERNAME>）はネットワーク関連の DLL と SYS ファイルを読み取る権限が必要です。

fsms_<COMPUTERNAME> のアカウントには、次のディレクトリを読み取れる権限を許可してください。

%SystemRoot%

%SystemRoot%¥system32

%SystemRoot%¥system32¥drivers

サービス制限の中では、F-Secure ポリシー マネージャ サーバ サービスの起動を拒否するものもあります。詳細については、Microsoft Windows サーバの取扱説明をご覧ください。

Q. F-Secure ポリシー マネージャ サーバに接続できません。

A. 「Unable to connect to management server. Another administrator may be logged on」のエラー メッセージが発生した場合、F-Secure ポリシー マネージャ コンソールから F-Secure ポリシー マネージャ サーバにログインしているユーザがいるかを確認してください。このエラーは F-Secure ポリシー マネージャ コンソールの不正なシャットダウンによって発生する可能性もあります。問題を解消するには、F-Secure ポリシー マネージャ サーバがタイムアウトするまで（<=5 分）待つか、Commdir にある admin.lck を削除して、F-Secure ポリシー マネージャ サーバのサービスを再開します。

Q. F-Secure ポリシー マネージャ コンソールと F-Secure ポリシー マネージャ サーバの接続が切断します。

A. F-Secure ポリシー マネージャ コンソールが F-Secure ポリシー マネージャ サーバとは別のコンピュータで動作している場合、ネットワークの問題で接続が影響される可能性があります。ネットワーク スイッチの変更などで、F-Secure ポリシー マネージャ コンソールとサーバの間で接続が失われた問題がいくつかあります。通常、このような問題は影響されているマシンのネットワーク ドライバを更新すること、または F-Secure ポリシー マネージャ コンソールとサーバの新しいスイッチとネットワーク カードを再設定することによって解消されます。

F-Secure ポリシー マネージャ コンソールが F-Secure ポリシー マネージャ サーバと同じコンピュータにインストールされている場合、F-Secure ポリシー マネージャ サーバのネットワーク負荷が多いため、利用可能のネットワーク接続が 1 つもない可能性があります。その結果、F-Secure ポリシー マネージャ コンソールとすべてのホストがネットワークの同じリソースを競合していることとなり

ます。また、Windows 95 のマシンがネットワークにある場合はさらなる注意が必要です。Windows 95 のマシンはネットワークを「開いた」状態で離れることがあることから、F-Secure ポリシー マネージャ サーバまたはコンソールでアクセスができない場合があります。

デフォルトの設定では、F-Secure ポリシー マネージャ サーバは最大 150 までの同時接続に対応できます。httpd.conf にある ThreadsPerChild の値をより高い数値に変更することによって、同時接続の最大数を増やせます。また、ホストのポーリング間隔を長くしたり、いくつかのホストをアンチウィルス プロキシに移動したり、Windows のネットワーク タイムアウト設定を短くしたり、Windows のネットワーク ポート数を増やしたりすることで、ネットワークの負荷を軽くすることができます。

下記の設定は本製品を効率的に使用するための Windows のネットワーク設定です。

HKLM¥SYSTEM¥CurrentControlSet¥Services¥Tcpip¥Parameters¥
MaxUserPort（ネットワークの最大ポート大数、デフォルト = 5000)

HKLM¥SYSTEM ¥CurrentControlSet¥Services¥Tcpip¥Parameters¥ TcpTimedWaitDelay（非アクティブのネットワーク接続を閉じるまでの待ち時間、デフォルト = 240 秒).

netstat -an のコマンドを使用すると、サーバへの接続数を確認できます。

A

SNMP サポート

概要 218
SNMP サポートを含む F-Secure 管理エージェントのインストール 219
SNMP マスター エージェントの設定 220
マネージメント インフォメーション ベース (MIB) . 221

A-1　概要

この付録では、SNMP サポートに関する以下のトピックを扱います。

- F-Secure 管理エージェントの SNMP エージェント
- SNMP サポートを含む F-Secure 管理エージェントのインストール
- F-Secure 管理エージェントの MIB（マネージメント インフォメーション ベース）
- F-Secure 管理エージェントによって送信される SNMP トラップ
- ネットワーク マネージャ ソフトウェア アドオン

SNMP サポートは、現在 Windows 2000 および Windows XP を含む Windows NT の全バージョンに実装されています。

A-1.1　F-Secure 管理エージェント用の SNMP サポート

Windows NT

F-Secure 管理エージェント用の SNMP サポート（NT バージョン）は、サービスとして Windows NT マスター エージェントを実装しています。SNMP サービスは、ネットワーク通信に Windows ソケットを使用するため、Windows ソケットが TCP/IP または IPX/SPX とともにインストールされている必要があります。

マスター エージェントは拡張可能な SNMP エージェントであり、追加 MIB サービスが可能になります。Windows NT の SNMP エージェント自体には、MIB 用のインスツルメンテーション機能はありません。代わりに、NT ワークステーションまたはサーバに対する SNMP 要求を取り出し、それらの要求を分析のために適切なモジュールに渡す役割を果たします。

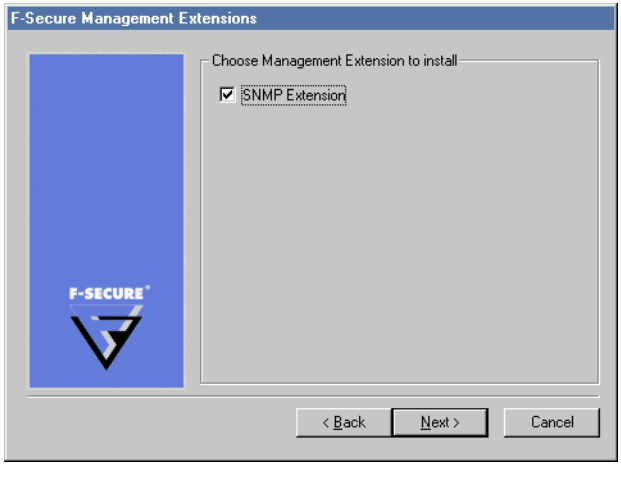
F-Secure SNMP 管理機能拡張は Windows NT の SNMP 機能拡張エージェントで、マスター エージェントでロードおよびアンロードされます。SNMP サービスは通常、Windows NT の起動時に起動します。したがって、拡張エージェントは常にロードされています。NT マスター エージェントは機能拡張を受け入れ、要求を管理エージェントに渡します。管理エージェントは、作成した管理コンソールにその要求を戻す役割を果た

します。F-Secure SNMP 管理エクステンションは、他のモジュールがロードされていない場合でもロードできます。したがって、F-Secure SNMP 管理エクステンションは、F-Secure 管理エージェントの動作を、他の F-Secure 管理エージェントのモジュールとは別に監視できます。

A.2 SNMP サポートを含む F-Secure 管理エージェントのインストール

A-2.1 F-Secure SNMP 管理エクステンションのインストール

F-Secure 管理エージェントの SNMP サポートは、管理エクステンションをインストールすることによってインストールされます。



F-Secure SNMP 管理エクステンションのインストール時に SNMP マスター エージェントをインストールする場合、対応する Service Pack を再インストールする必要があります（『SNMP マスター エージェントの設定』を参照してください）。

A.3 SNMP マスター エージェントの設定

SNMP サービスは、Windows の［コントロール パネル］->［ネットワーク］ウィンドウからインストールされます。SNMP サービス オプションは、TCP/IP のインストール オプションのウィンドウにあります。SNMP サービス ソフトウェアがコンピュータ上にインストールされたら、SNMP を機能させるため、有効な情報で設定する必要があります。

SNMP を設定するには、ローカル コンピュータの管理者としてログオンする必要があります。SNMP 設定情報はコミュニティとトラップの送信先を定義します。コミュニティは SNMP サービスを実行する Windows NT コンピュータが属しているホストのグループです。トラップの送信先のコミュニティを 1 つまたは複数指定できます。コミュニティ名はトラップに含まれます。

正しいコミュニティ名が含まれておらず、サービスの許可済みのホスト名と一致しない情報要求を SNMP サービスが受信すると、SNMP サービスはトラップの送信先にトラップを送信し、要求が認証されなかったことを示します。

トラップの送信先には、選択したコミュニティ名が含まれたトラップを SNMP サービスによって送信する対象のホストを、名前または IP アドレスで指定します。

SNMP を統計に使用するが、コミュニティやトラップを識別しない場合は、SNMP サービスの設定時に「public」のコミュニティ名を指定できます。

SNMP の［セキュリティの構成］ダイアログ ボックスを使用して、SNMP サービスのセキュリティ パラメータを指定します。このダイアログ ボックスは、[SNMP サービスの構成］ダイアログ ボックスの［セキュリティ］ボタンをクリックすると表示されます。

SNMP のセキュリティで、コンピュータが要求を受け付けるコミュニティとホストを指定し、未認証のコミュニティやホストの情報要求時に認証トラップを送信するかどうかを指定できます。

A.4 マネージメント インフォメーション ベース (MIB)

マネージメント インフォメーション ベース (MIB) では、SNMP エージェントの、一連の管理されているオブジェクトが記述されています。管理システムは、SNMP エージェントが拡張エージェント DLL をその MIB に関連付けた場合にオブジェクトを操作できます。

SNMP MIB ファイルは、F-Secure ポリシー マネージャ コンソールのインストール時に、F-Secure ポリシー マネージャ コンソールの Administrator¥snmp mib¥ に自動的にインストールされます。各製品固有の SNMP MIB ファイルがあります。

管理されている各オブジェクトのエントリには、固有の識別子 (OID) があります。エントリには、オブジェクトのタイプ（カウンタ、文字列、ゲージ、アドレスなど）、オブジェクトのアクセス タイプ（読み取り、読み取り / 書き込みなど）、サイズ制限、範囲情報も含まれています。

OID は、特定のオブジェクトに割り当てられた一意の識別子です。識別子は、オブジェクト自体とオブジェクトのソースを識別する一連の数字で構成されます。OID はツリー構造で構成され、数列によって、特定のオブジェクトのソースであるサブツリーのさまざまなブランチが識別されます。ツリーのルートは、ISO（国際標準化機構）のトランクで、値は 1 です。ルートの下の各ブランチによって、特定のオブジェクトのソースを確認できます。SNMP オブジェクトは、iso.org.dod.internet または 1.3.6.1 で識別されたブランチのメンバーです。ドット表記の追加要素によって、オブジェクトの正確な場所がさらに指定されます。各サブブランチの数字は、すべてのブランチが一意となるように IETF により割り当てられます。

トラップは、エージェントから事前設定済みの管理ステーションへの SNMP メッセージです。重要なイベントを管理コンソールに通知するのに使用されます。通常、トラップはサービスの開始と停止のレポート、重大なエラー状態のレポートなどに使用されます

トラップは、F-Secure ポリシー マネージャ コンソール内の製品のリダイレクト テーブルで転送が選択されている場合のみ、SNMP エージェントを通じて管理ステーションに送信されます。トラップのリダイレクトの詳細については、『警告転送の設定』(P142) を参照してください。

B llaunchr のエラー コード

概要 224
エラー コード 225

B.1 概要

サイレント モードで実行した llaunchr.exe が完了すると、インストールの結果が標準の終了コードで報告されます。ログイン スクリプトを使用して、問題の原因をテストできます。ログイン スクリプトに指定可能なコマンドの例を以下に示します。

```
Start /Wait lLaunchr.exe ¥¥server¥share¥mysuite.jar /U
if errorlevel 100 Go to Some_Setup_Error_occurred
if errorlevel 5 Go to Some_llaunchr_Error_occurred
if errorlevel 3 Go to Problem_with_JAR_package
if errorlevel 2 Go to User_does_not_have_admin_rights
if errorlevel 1 Go to FSMA_was_already_installed
if errorlevel 0 Echo Installation was OK!
```

B.2 エラー コード

0	インストールは正常に完了しました。
1	FSMA はすでにインストールされています。
2	ユーザに管理者権限がありません。
3	JAR が見つかりません。
4	JAR が壊れています。
6	インストール パッケージの解凍中にエラーが発生しました。
7	インストール先ディスクに十分な空き容量がありません。
8	package.ini が JAR ファイルの中にありません。
9	package.ini に作業手順がありません。
10	コマンドラインまたは .ini ファイルに不正なパラメータがあります。
11	新しい作業プロセスの初期化中にエラーが発生しました。
12	セットアップ用インストール手順の作成中にエラーが発生しました。
13	一時ディレクトリを作成できませんでした。
14	未知のエラーです。
100	サイレント モードでインストールするのに必要なデータが不足しています。無効な JAR ファイルです。

101	更新は無効になっています（セットアップはインストールを更新しようとしました）。
102	product.ini を読み取れませんでした。
103	prodsett.ini で無効なデータが検出されました。
104	管理エージェントによりインストールがキャンセルされたか、競合するソフトウェアが検出されました。インストールは中止されました。
105	入力した CD キーが間違っているか、CD キーが入力されていません。インストールは中止されました。
110	ディスクの空き容量が不足しています。
111	インストール先ドライブはローカル ドライブではありません。
120	マシンに対する管理者権限を持っていません。
130	解凍したファイルをインストール先ディレクトリにコピーできませんでした。
131	アンインストール プラグインを製品のインストール先ディレクトリにコピーできませんでした。
132	product.ini ファイルを一時ディレクトリにコピーできませんでした。
133	製品ファイルのインストール先ディレクトリへのコピー中にエラーが発生しました。
134	prodsett.ini をコピーできません。
140	新しいバージョンのスイートが検出されました。
150	製品のプラグイン dll をロードできませんでした。

151	インストール サポート dll をロードできませんでした。
152	ラッパー dll をロードできませんでした。
160	キャビネット ファイルを初期化できませんでした。
170	管理エージェントのセットアップ プラグインがエラーを返しました。
171	プラグインが予期しないコードを返しました。
172	プラグインがラッパー コードを返しました。
173	前回のインストール操作またはアンインストール操作が完了していません。操作を完了するには再起動する必要があります。
174	以前のインストール操作またはアンインストール操作を完了させるために、インストール先に指定したマシンが再起動されました。インストール情報を再送信してください。
200	部分的に成功しました。一部の製品のインストールは失敗しました。

C

FSII リモート インストールのエラー コード

概要 230
Windows エラー コード 230
エラー メッセージ 231

C.1 概要

この付録では、「Windows ホストの自動検出」の動作時に発生する可能性のある最も一般的なエラー コードおよびメッセージについて説明します。

C.2 Windows エラー コード

エラー コード	説明
1057	ユーザ アカウント名が無効であるか、存在しません。
5	アクセスは拒否されました。[このアカウント] を使用している場合、管理者は F-Secure ポリシー マネージャ コンソール マシンにドメイン管理者権限でログインする必要があります。ドメインの信頼レベルで、信頼済みドメインのアカウントを使用して F-Secure ポリシー マネージャ コンソールにログインしていることを確認してください。
1069	ログイン失敗。ほとんどの場合、入力したパスワードが間違っています。
1722	RPC サーバを利用できません。このエラー メッセージは、インストール直後にホストを再起動したために、インストールが正常に完了したかどうか F-Secure ポリシー マネージャ コンソールが確認する時間がなかった場合に表示されることがあります。
1219	F-Secure ポリシー マネージャ コンソールが、インストール先のワークステーションへのネットワーク接続を確立しています。別のユーザ アカウントで接続を確立する前に、この接続を切断してください。

C.3 エラー メッセージ

Q. 必要な権限が現在のアカウントに与えられていません。必要な権限を手動で割り当てる必要があります。

A. デフォルトでは、管理者でさえも F-Secure ポリシー マネージャ コンソール マシン上で必要な「オペレーティング システムの一部として機能」権限を持っていません。この権限を持っていない場合、Windows NT は、入力したユーザ アカウントを FSII が認証するのを許可しません。F-Secure ポリシー マネージャ コンソール上の管理者のアカウントにこの権限を追加するには、Windows NT の［ユーザ マネージャ］->［原則］->［ユーザの権利］を使用します。

Q. 管理エージェントによりインストールがキャンセルされたか、競合するソフトウェアが検出されました。インストールは中止されました。

A. 以下の場合に、セットアップの一部である管理エージェントによりインストール全体がキャンセルされます。

1. 競合するサードパーティ製ソフトウェアが検出された場合
2. 以下のいずれかの設定パラメータが間違っている場合
   - 通信ディレクトリのパス
   - 通信アカウントまたはパスワード
   - ポリシー マネージャ サーバへの URL

Q. 入力した CD キーが間違っているか、CD キーが入力されていません。インストールは中止されました。

A. 入力した CD キーが間違っているため、リモート ホストでインストールを開始できません。構文を確認してください。

Q. インストール先ホストのディスク空き容量が不足しています。

A. インストール先ホストに十分なディスク空き容量がありません。通常、少なくとも 20MB 必要です。

Q. 重大な FSMAINST エラーにより、管理エージェントのインストールが失敗しました。詳細については、ホスト ログ ファイルを参照してください。

A. F-Secure 管理エージェントのインストール中に、重大なインストール エラーが発生しました。管理エージェントを手動でホストにインストールすることをお勧めします。fswssdbg.log ファイルの ERROR キーワードを参照して、詳細情報を確認できます。このファイルは、インストール先ホストの Windows ディレクトリにあります。

Q. F-Secure 製品の新しいバージョンが検出されました。インストールを中止します。

A. インストール先のホストに新しいバージョンの製品がインストールされている場合は、それをアンインストールしてからでないとインストールを実行できません。

Q. prodsett.ini で無効なデータが検出されました。

A. prodsett.ini 環境設定ファイルの情報が間違っています。手動で編集した場合は、構文が正しいことを確認してください。
prodsett.ini を直接編集するのではなく、JAR ファイルをエクスポートし、ILAUNCHR を使用してインストールしてください。

D Windows 98/ME でのリモート インストールのサポート

リモート管理の有効化 234

D.1 リモート管理の有効化

Windows 98/ME を使用しているワークステーションで FSII を使用するためには、ワークステーションでいくつかの設定を行う必要があります。リモート管理できるようにするには、次の手順を実行します。

1. ［コントロール パネル］-［ネットワーク］の順に選択し、ファイルの共有を有効にします。
2. ［コントロール パネル］-［ネットワーク］ダイアログ ボックスの順に開き、ユーザ アカウント関連のセキュリティを有効にします。
3. ［コントロール パネル］-［パスワード］の順に選択し、リモート管理が有効になっていることを確認します。

オプションのリモート レジストリのサポート

F-Secure ポリシー マネージャ コンソールの自動検出画面に、インストールされているエージェントのバージョンを表示したい場合は、次の手順を実行して Microsoft 98/ME リモートレジストリ サービスをインストールする必要があります。

1. ［コントロール パネル］-［ネットワーク］の順に選択し、［ネットワーク］ダイアログ ボックスで［ネットワークの設定］タブを選択して［追加］をクリックします。
2. ［ネットワーク コンポーネントの選択］ダイアログ ボックスで［サービス］をダブルクリックします。
3. ［ネットワーク サービスの選択］ダイアログ ボックスで［ディスク使用］をクリックします。
4. ［ディスクからインストール］ダイアログ ボックスに Windows 9x CD-ROM へのパス「ADMIN¥NETTOOLS¥REMOTREG」を入力して［OK］をクリックします。
5. ［ディスクからインストール］ダイアログ ボックスで［OK］をクリックします。
6. ［ネットワーク サービスの選択］ダイアログ ボックスで［Microsoft リモート レジストリ］をクリックし、［OK］をクリックします。

FAQ

Q. Windows 9x でリモート管理を適切に有効にしましたが、FSII を使用しようとすると、常にエラー 5（アクセス拒否）が返されます。

A. [リモート管理] ページ（[コントロール パネル] の [パスワード] ダイアログ）で、[Administrators] リストにドメイン管理者のアカウント / グループの正しい名前が含まれていることを確認してください。デフォルトでは、英語版以外の Windows 9x マシン（日本語、フィンランド語など）には、英語版の Windows NT Server とは互換性のない間違ったユーザ グループ名が含まれています。[Administrators] リストに、英語のみの管理者グループ名 (Domain Admins) が含まれることを確認してください。

E

ネットマスクに使用する NSC 表記

概要 238

E.1 概要

NSC 表記は、ネットワーク アドレスとその関連するネットマスクを組み合わせた、標準の簡略表記です。

NSC 表記は、ネットマスク内で隣接する 1 ビットの数を、ネットワーク アドレスの後にスラッシュと数字を使用して定義します。簡単な例を以下に示します。

ネットワーク アドレス	ネットマスク	NSC 表記
192.168.0.0	255.255.0.0	192.168.0.0/16
192.168.1.0	255.255.255.0	192.168.1.0/24
192.168.1.255	255.255.255.255	192.168.1.255/32

NSC 表記は、1 が立っているビットが連続することのない「櫛」状のネットマスクを使用するネットワークでは使用できません。以下の表に、許可された各ネットマスクのビット数を示します。

0.0.0.0/0 は、デフォルト ルート用に予約された特殊なネットワーク定義です。

ネットマスク	ビット数	ネットマスク	ビット数
128.0.0.0	1	255.128.0.0	9
192.0.0.0	2	255.192.0.0	10
224.0.0.0	3	255.224.0.0	11
240.0.0.0	4	255.240.0.0	12
248.0.0.0	5	255.248.0.0	13
252.0.0.0	6	255.252.0.0	14
254.0.0.0	7	255.254.0.0	15
255.0.0.0	8	255.255.0.0	16

ネットマスク	ビット数	ネットマスク	ビット数
255. 255. 128. 0	17	255. 255. 255. 128	25
255. 255. 192. 0	18	255. 255. 255. 192	26
255. 255. 224. 0	19	255. 255. 255. 224	27
255. 255. 240. 0	20	255. 255. 255. 240	28
255. 255. 248. 0	21	255. 255. 255. 248	29
255. 255. 252. 0	22	255. 255. 255. 252	30
255. 255. 254. 0	23	255. 255. 255. 254	31
255. 255. 255. 0	24	255. 255. 255. 255	32

テクニカル サポート

概要 242
Web Club 242
高度なテクニカル サポート 242
F-Secure 製品技術研修 243

概要

F-Secure のテクニカル サポートは電子メールまたは F-Secure の Web サイトでご利用いただけます。Web サイトには、F-Secure アプリケーション内から、または Web ブラウザからアクセスできます。

Web Club

F-Secure Web Club は、F-Secure 製品のユーザをサポートをします。アクセスするには、F-Secure アプリケーションの［ヘルプ］メニューから［Web Club］を選択します。初めてこのオプションを使用する場合、Web ブラウザのパスと名前、および自分の地域を入力します。

Web ブラウザから Web Club に直接接続するには、以下のサイトにアクセスします。

http://www.f-secure.com/webclub/

Web 上でのウィルス説明

F-Secure Corporation は Web サイトにウィルス関連の総合的な情報を保有しています。ウィルス情報データベースを表示するには、次の URL にアクセスします。

http://www.f-secure.com/virus-info/

高度なテクニカル サポート

高度なテクニカル サポートについては、F-Secure サポート センター（http://support.f-secure.com/）にアクセスするか、または F-Secure の販売代理店に直接お問い合わせください。

基本的なテクニカル サポートについては、F-Secure の販売代理店にお問い合わせください。

サポートの要求時には、以下の情報を明記してください。

1. お使いの F-Secure ソフトウェア プログラムの名前とバージョン番号（ビルド番号も含む）。
2. お使いのオペレーティング システムの名前とバージョン番号（ビルド番号も含む）。
3. 問題に関する詳しい説明（プログラムによって表示されるエラーメッセージや、問題の再現に役立つその他の状況など）。

電話で F-Secure Corporation のサポートを受ける場合は、効率よく短時間でサポートを行うため以下の準備を行ってください。

- サポート技術者の説明にしたがって操作ができるようにコンピュータの前にいるか、または説明をメモする準備をします。
- お使いのコンピュータを起動させ、可能であれば、問題が発生した状態にしてください。または、コンピュータですぐに問題を再現できるように準備してください。

F-Secure ソフトウェアをインストールすると、F-Secure プログラム フォルダに ReadMe ファイルが含まれています。このフォルダは、Windows の［スタート］メニューから［プログラム］を選択すると表示されます。ReadMe ファイルには、この製品に関する最新情報が記載されています。

F-Secure 製品技術研修

F-Secure では製品技術研修、教材、情報を販売代理店やお客様に提供し、F-Secure のセキュリティ製品およびサービスの取り扱いが支障なく進むようにしています。研修については F-Secure 認定研修パートナーによる提供も行っています。これらのツールや専門家の活用により、パートナーは企業のセキュリティを独自の強力なソリューションで実現し、競合他社に差をつけることができます。さらに、顧客満足度をより高めて、マーケット シェアと収益性を向上させることもできます。

研修プログラム

研修プログラムの詳細については、インターネットで次の URL にアクセスして、F-Secure 製品技術研修のページを参照してください。

http://www.f-secure.com/products/training/

研修には新しく設備の充実した教室を使用します。研修は理論説明と実習で構成されています。各コースの最後には認定試験があります。コースの内容とスケジュールについては、お近くの F-Secure 営業所または F-Secure 認定研修パートナーにお問い合わせください。

問い合わせ先

全般 ：Training@f-secure.com

登録 ：Training-Registration@f-secure.com

フィードバック ：Training-Feedback@f-secure.com

用語集

認証

自分の身元を証明すること。

認可

あるオブジェクトに対してある操作を実行する権利。また、この権利を証明すること。

ビット

メモリ サイズの最小単位で、ビットの集合がバイトを構成します。連続したパターンに配列されることにより、コンピュータの処理システムによって認識可能な文字、数値、またはその他の詳細情報を表します。

バイト

1 つの文字を表すビットの集合。1 バイトは 8 ビットで構成されます。

証明書

「公開鍵」を参照。

クライアント

別のコンピュータ上のサーバ プログラムにアクセスしてデータを取得するために使用されるプログラム。

破損

ユーザの許可または承認なしに変更されたデータ。

ドメイン名

インターネット サイトを識別する固有の名前（例 : F-Secure.com）。

DNS

Domain Name System（ドメイン ネーム システム）。ノードの識別名を IP アドレスに変換するサービス。DNS は分散型データベースを使用します。

ファイアウォール

セキュリティ上の目的からネットワークを 2 つ以上のセグメントに分割するための、ハードウェアとソフトウェアの組み合わせ。

FTP

File Transfer Protocol（ファイル転送プロトコル）。2 つのインターネット サイト間でファイルを転送するために一般的に使われている方法。

ホスト

ネットワーク上の他のコンピュータが利用できるサービスのリポジトリである、ネットワーク上のコンピュータ。

HTTP

Hyper Text Transfer Protocol（ハイパー テキスト転送プロトコル）。ドキュメントを要求し、その内容を転送するために、Web ブラウザとサーバ間で使用されるプロトコル。HTTP の仕様は、World Wide Web コンソーシアムによって管理されています。

IP アドレス

Internet Protocol アドレス。ドットによって区切られている 4 つの数値から構成される固有のネットワーク アドレス。IPv6 から形式が変更されます。

IPSec

(IETF) IP Security Protocol（IP セキュリティ プロトコル）。IPv4 および IPv6 に、相互運用可能な高品質の暗号化ベースのセキュリティを提供することを目的に定められています。このプロトコルによって提供されるサービスには、アクセス制御、コネクションレスの保全性、データ元の認証、リプレー防止、秘密性（暗号化）、およびトラフィック フローの制限付き秘密性などがあります。これらのサービスは IP 層で実装され、IP および上層プロトコルに対する保護を提供します。

ISP

Internet Service Provider（インターネット サービス プロバイダ）。何らかの形態でインターネットへのアクセスを提供する機関。

JAR

Java ARchive。複数のファイルを 1 つにまとめるために使用されるファイル形式。

カーネル モード

Windows オペレーティング システムの一部。特にユーザ モードのアプリケーションとサービスは、カーネル モードを通じ、API を使用してコンピュータのハードウェアと対話します。また、カーネル モードにはユーザ モードへのインタフェースと、専用のサービスを同期してすべての I/O 機能を調整する機能も含まれます。カーネル モード メモリは、ユーザ モードのアクセスから保護されます。

LAN

Local Area Network（ローカル エリア ネットワーク）。同じビルまたは同じ階など、物理的に近い地域に限られたコンピュータ ネットワーク。単純なネットワーク プロトコルを使用することもあります。

ログイン（名詞）

コンピュータ システムにアクセスするために使用するアカウント名。

Mbit

メガビット。

MD5

Message Digest number 5（メッセージ ダイジェスト ナンバー 5）。RFC 1321 で公開されているセキュア ハッシュ関数。

MIB

(SNMP の用語）Management Information Base（マネージメント インフォメーション ベース）。MIB の詳細情報については、RFC1155-SMI、RFC1212-CMIB、および RFC1213-MIB2 を参照してください。

ネットマスク

IP アドレスがどのようにネットワーク部とホスト部に分かれているかを示します。

ネットワーク

リソースを共用するために接続された 2 台以上のコンピュータ。2 つ以上のネットワークが接続されたものがインターネットです。

Ping

ICMP エコー パケットを送信し、エコー返信パケットを受信することにより、リモート コンピュータへの接続を検証すること。

ポリシー

ユーザがシステムのリソースにアクセスできる条件をまとめたもの。

ポリシーベース管理

ポリシー文を使用してシステムの動作と設定を制御すること。

秘密鍵

公開鍵システムで使用される鍵のうち、公開されずに所有者によってのみ使用されるもの。これは、メッセージの復号化や電子署名の作成に使用される鍵です。

プロトコル

複数の対象によって実行されるアルゴリズムまたは段階的な手順。

公開鍵

公開鍵システムの鍵のうち、広く配布される（保護されない）もの。この鍵は暗号化（復号化ではない）または署名の確認に使用されます。公開鍵には、所有者、発行元、有効期間などに関するその他の情報も含まれています。

乱数シード

暗号の強度が高い乱数ジェネレータに対するシード値で、F-Secure アプリケーションが終了するたびに更新されます。

サーバ

クライアント ソフトウェアに対して特定のサービスを提供するコンピュータまたはソフトウェア。

サービス

誰がログインしているかにかかわらずホスト上で実行され、その他のアプリケーションにサービスを提供するアプリケーション。

SNMP

Simple Network Management Protocol（簡易ネットワーク管理プロトコル）。LAN または WAN に接続されたリピータ、ブリッジ、ルータ、およびその他のデバイスのネットワーク パラメータやカウンタを監視および設定するために使用される標準 TCP/IP プロトコル。

TCP/IP

Transmission Control Protocol/Internet Protocol（伝送制御プロトコル / インターネット プロトコル）。インターネットを定義するプロトコル スイートです。元々は UNIX オペレーティング システム用に開発されたものですが、現在はほとんどの主要なコンピュータ オペレーティング システムに対する TCP/IP ソフトウェアが提供されています。インターネットを使用するためには、コンピュータに TCP/IP ソフトウェアが必要です。

テキスト ファイル

ASCII 文字またはラテン印刷可能文字を含む 1 つ以上の行の連続として解釈されるように作成されたファイル。

URL

Uniform Resource Locator（ユニフォーム リソース ロケータ）。インターネット上のリソースのアドレスを指定するための標準的な方法です。

ユーザ モード

ユーザ アプリケーションを実行し、オペレーティング システムの機能を実行するためにカーネル モードを呼び出す、オペレーティング システム内の保護された部分。

パターン ファイル

パターン ファイルはウィルスの検出に使用されます。新しいウィルスが発見された場合は、ウィルス保護がそのウィルスを検出できるようにパターン ファイルを更新する必要があります。

VPN

Virtual Private Network（バーチャル プライベート ネットワーク）。既存のインターネットを使用した安全な私設ネットワーク。

WAN

Wide Area Network（ワイド エリア ネットワーク）。インターネット、あるいは 1 つのビルまたはキャンパスより広い地域を範囲とするネットワーク。

F-Secure Corporation について

F-Secure は 2004 年に 50% の収益成長率を遂げ、アンチウィルスおよびコンピュータ セキュリティ業界で株式公開されている企業で目覚しい成長を記録している企業です。1988 年に設立された F-Secure は 1999 年からヘルシンキの証券取引所に上場しており、フィンランドのヘルシンキに本社を置くほか、米国、フランス、ドイツ、スウェーデン、イギリス、日本など全世界で 14 のオフィスがあり、100 カ国以上のサービス パートナー、付加価値再販業者および販売代理店を通じてサービスを提供しています。F-Secure の保護サービスは、Nokia などのモバイル端末メーカ、およびドイツテレコム、フランステレコム、Charter Communications などの大手インターネット サービス プロバイダのサービスを通じてもご利用できます。最新のリアルタイム ウィルス情報は、F-Secure アンチウィルス研究チームの研究所ブログでご覧になれます（英文）。
http://www.f-secure.com/weblog/

個人および企業向けのサービス

F-Secure のサービスとソフトウェアは個人および企業をコンピュータ ウィルスとインターネットまたはモバイルのネットワークから発生するセキュリティの脅威から保護します。受賞歴のあるソリューションは、アンチウィルス、侵入防止機能を備えたデスクトップ ファイアウォール、アンチスパム、およびスパイウェア対策ソリューションを含めています。F-Secure の一番の強みは、新しい脅威に対する応答速度にあります。企業のお客様には、集中管理が可能で、優れた連携機能を備えたワークステーションおよびサーバ向けのソリューションを提供しています。セキュリティの専門技術を組織内で構築したくない企業には、提携会社を介してセキュリティのサービスを代わりに提供することもできます。

F-Secure の製品とサービスの詳細については、http://www.f-secure.com/products/ をご覧ください。